PROGUARD800™ SERIES
INSTALLATION MANUAL

ENGLISH

20195 / 20080318 • PROGUARD800™
© ALL RIGHTS RESERVED MARMITEK ®

MARMITEK®

Safety Warnings

• The wiring of your electrical installation is live (230 V) and extremely dangerous. Never connect the module when plugged into the mains. Always turn off the main switch before starting the installation.

• This product is for professional use and should be installed by a certified installer.

• To prevent short circuits, this product should only be used inside and only in dry spaces. Do not expose the components to rain or moisture. Do not use the product close to a bath, swimming pool etc.

• Do not expose the components of your systems to extremely high temperatures or bright light sources.

• In case of improper usage or if you have altered and repaired the product yourself, all guarantees expire. Marmitek does not accept responsibility in the case of improper usage of the product or when the product is used for purposes other than specified. Marmitek does not accept responsibility for additional damage other than covered by the legal product responsibility.

• This product is not a toy. Keep out of reach of children.

• Keep batteries out of the reach of children. Dispose of batteries as chemical waste. Never use old and new batteries or different types of batteries together. Remove the batteries when you are not using the system for a longer period of time. Check the polarity (+/-) of the batteries when inserting them in the product. Wrong positioning can cause an explosion.

• Only connect the adapter to the mains after checking whether the mains voltage is the same as the values on the identification tags. Never connect an adapter or power cord when it is damaged. In that case, contact your supplier.

• Automatic switching devices provide comfort, but can also be dangerous. They can surprise people or can ignite clothing hanging over an electric heat source. Please be careful and take appropriate measures to avoid accidents.

© MARMITEK

Table of Contents

Safety Warnings 2
Table of Contents 3
Chapter One: Introduction 6
1.1: Documentation Conventions 6
1.2: Specifications 7
1.3: System Overview 7
1.4: Hardware Layout 9
Chapter Two: System Installation 13
2.1: Pre-Installation Planning 13
2.2: Installation Procedure 14
2.3: Back Tamper 17
2.4: Installing HK855 Hardwire LCD Keypads 17
Chapter Three: Basic System Operation 19
3.1: Front Panel Layout 19
3.2: System Status LEDs 19
3.3: Front Panel Keypad 20
3.4: LCD Display 20
3.5: Vocal Message Annunciation 21
3.6: HK855 Hardwire LCD Keypad 22
3.7: Arming/Disarming 23
3.8: Remote Arming/Disarming via SMS 25
3.9: Remote Arming/Disarming via DTMF 26
3.10: LCD Keypad Alarm Activation 26
Chapter Four: Advanced System Operation 28
4.1: Menu Navigation 28
4.2: Stop Communications 28
4.3: Sensor Bypassing/Unbypassing 29
4.4: User Codes 29
4.5: Follow Me 31
4.6: Event Log 31
4.7: Service Menu 32
Chapter Five: Telecontrol and Two-Way Audio 37
5.1: Incoming Calls 37
5.2: Outgoing Calls 39
Chapter Six: X-10 Home Automation Control 42
6.1: Keypad Control 42
6.2: Keyfob Control 42
6.3: Telephone Control 42
6.4: Scheduling 43
Chapter Seven: Devices 45
7.1: Device Registration 45
7.2: Device Descriptors 45
7.3: Device Deletion 45
7.4: Supervision Time 46
7.5: Re-Synchronization 46
7.6: Zones 46
7.7: Keyfobs 49
7.8: Keypads 50
7.9: Repeaters 51
7.10: Wireless Siren 51
7.11: Smartkeys (for future use) 52
Chapter Eight: Entry/Exit Timers and System Tones 53
8.1: Entry/Exit Delay 53
8.2: Arm on Exit 53
8.3: Supplementary Entry Delay 53
8.4: Entry Deviation 54

8.5: Exit Restart....54
8.6: Arming Tones....54
8.7: Home Automation Tones....55
8.8: System Trouble Tones....55
8.9: Tones Options....56
Chapter Nine: System Options....57
9.1: Swinger Setting....57
9.2: Code Lockout....57
9.3: Arm/Disarm Options....57
9.4: Panic Alarm....59
9.5: AC Loss Delay....59
9.6: Display Options....60
9.7: PGM Output Options....61
9.8: Guard Code (for future use)....62
9.9: “No Arm” Indication....62
9.10: Jamming Detection....62
9.11: “No Motion” Time....63
9.12: Microphone/Speaker Options....63
9.13: Vocal Messages....63
9.14: Installer Access....63
9.15: Auto Log View (for future use)....63
9.16: Daylight Savings....64
9.17: Report Fail Trouble....64
9.18: Cancel Alarm....64
9.19: Cross Zoning (for future use)....65
9.20: Verified Fire....65
9.21: Battery Type....65
Chapter Ten: Communications....66
10.1: Monitoring station Reporting....66
10.2: General Options for Monitoring station Reporting....67
10.3: Vocal Message Dialler....68
10.4: Remote Programming....70
10.5: Service Call....72
10.6: Communications Options....72
10.7: GSM Options....75
10.8: TWA Event Report Options....76
10.9: Event Options for Monitoring station Reporting....77
10.10: Vocal Message Dialler Event Options....78
Chapter Eleven: X-10 Home Automation Programming....80
11.1: X-10 Overview....80
11.2: HA Units....80
11.3: House Code....83
11.4: HA Control....83
Chapter Twelve: System Initialization....84
12.1: Initialization....84
12.2: Default Program Restore....84
12.3: Clear User Codes....84
12.4: Clear Wireless Transmitters....85
12.5: Find Modules....85
Appendix A: Menu Structure....86
Appendix B: Transmitter Installation....93
PIR Sensors (MS845)....93
Magnetic Contact (DS831)....96
Universal Transmitter (US832)....98
Glass break Sensor (GB843)....99
Smoke Detector (SD833)....102
Keyfobs (PR811/KR814)....103
Wireless Keypads (WK820/RC840)....104

© MARMITEK

Transmitter Specifications 106
Appendix C: Event Table 107
Appendix D: Zone Types 109
Declaration of Conformity 111

Chapter One: Introduction

This manual is designed to help you install the *ProGuard800* control panel. We strongly urge you to read through this manual, in its entirety, before beginning the installation process so that you can best understand all that this security system has to offer. This manual is not intended for end user use. End users are encouraged to read the user manual provided with the system. If you have any questions concerning any of the procedures described in this manual please look at www.marmitek.com.

1.1: Documentation Conventions

Throughout the manual, we have tried to include all of the operating and programming functions using a similar structure and order as they appear in the menu. A detailed explanation of how to navigate the panel's menu is included in section 4.1: Menu Navigation. In order to simplify the procedures that appear in the rest of this manual, the following conventions are used:

This…	**Means…**
Select…	Use the arrow keys to scroll through the options and press ✓.
From the Event Log Menu, select Clear Log.	Enter the main menu by pressing ✓ and entering your user code. Using the arrow keys, navigate until you reach Event Log and press ✓. Using the arrow keys, navigate until you reach Clear Log and press ✓.
From the Service menu, select Time/Date, Set Date.	The same as above only this time you are navigating through three menu levels.
[7012]	The shortcut to a specific menu item from the main menu. In this case, this is the shortcut for Set Date. These appear in the procedures as an additional aid to menu navigation.
[#5]	A shortcut to a specific item in a sub-menu. For example, [#5] is the shortcut to Bell enable disable in the sub-menu that is opened once you have selected the sensor you want to program.
✓	The symbol on a key that appears on the keypad
5. Interface Test	The text that actually appears on the LCD display (bold italics).
	Important note, please pay attention.

Table 1.1: Documentation Conventions

© MARMITEK

1.2: Specifications

General

Zones: 32 wireless zones (1 transmitter per zone), 1 hardwire zone (Zone 33)
Wireless Keyfobs: 19 (Controlled or Non-controlled)
Wireless Keypads: 4
HK855 Hardwire LCD Keypads: 2 (PROGUARD800-KPD/L), 3 (PROGUARD800-KPD/S)
Repeaters: 4
Smartkeys (future option): 16 (Controlled or Non-controlled)
Wireless Siren: 1 (1-way or 2-way)
User Codes: 32
Arming Methods: Full, Part or Perimeter
Event Log: 256 event capacity, time and date stamped

Communications

Monitoring station Event Reporting Accounts: 3 (8-digit account number)
Vocal Message Accounts: 3
Telephone Numbers: 3 regular, 3 Vocal Message, RP Callback and Service Call (16-digits each)
Communication Interface Options: PSTN or GSM (optional expansion module required)

Home Automation

Control Medium: Power-line carrier
Protocol: X-10
HA Units: 16 individually addressed

Receiver

Type: Super-heterodyne, fixed frequency
Frequency: 868.35 MHz FM
Data Encryption: SecuriCode™

Electrical

Power Input: 230VAC, 50Hz
Backup Battery Pack: 7.2V/1.5Ah (6 x 1.2V Ni-MH rechargeable cells, size AA)
Fuse Ratings: 63mA/250V (AC protection fuse), 1A/250V (battery protection fuse)
PGM Relay Output Contact Rating: 100mA (max. load)
Built-in Siren: 105dB or 85dB
Tamper Switch: N.C.
Operating Temperature: 0-60°C

1.3: System Overview

The *ProGuard800* is a full-featured wireless control panel that is expected to provide a solution to the needs of most residential installations. This system has been developed based upon a design concept geared towards easy installation and use. With this in mind, the user interface is based on a simple, menu-driven model that suits the essential requirements of both the user and installer alike. You can program the *ProGuard800* on-site using the on-board LCD keypad or off-site via a PC using the up/downloading software.

Monitoring station communication and up/downloading employ either regular PSTN or high-speed cellular communication. SMS messaging provides an innovative method used for both monitoring station and Follow-me user monitoring. Additionally, SMS messages can be sent to the panel enabling the user to send commands to the system from anywhere on the planet.

The panel's home automation capabilities provide a wealth of features. The Home Automation module interfaces with X-10 units over the powerline network and grants the user appliance control via a number of different media.

The following diagram shows the components that make up the system and the system's interaction with external communication networks.

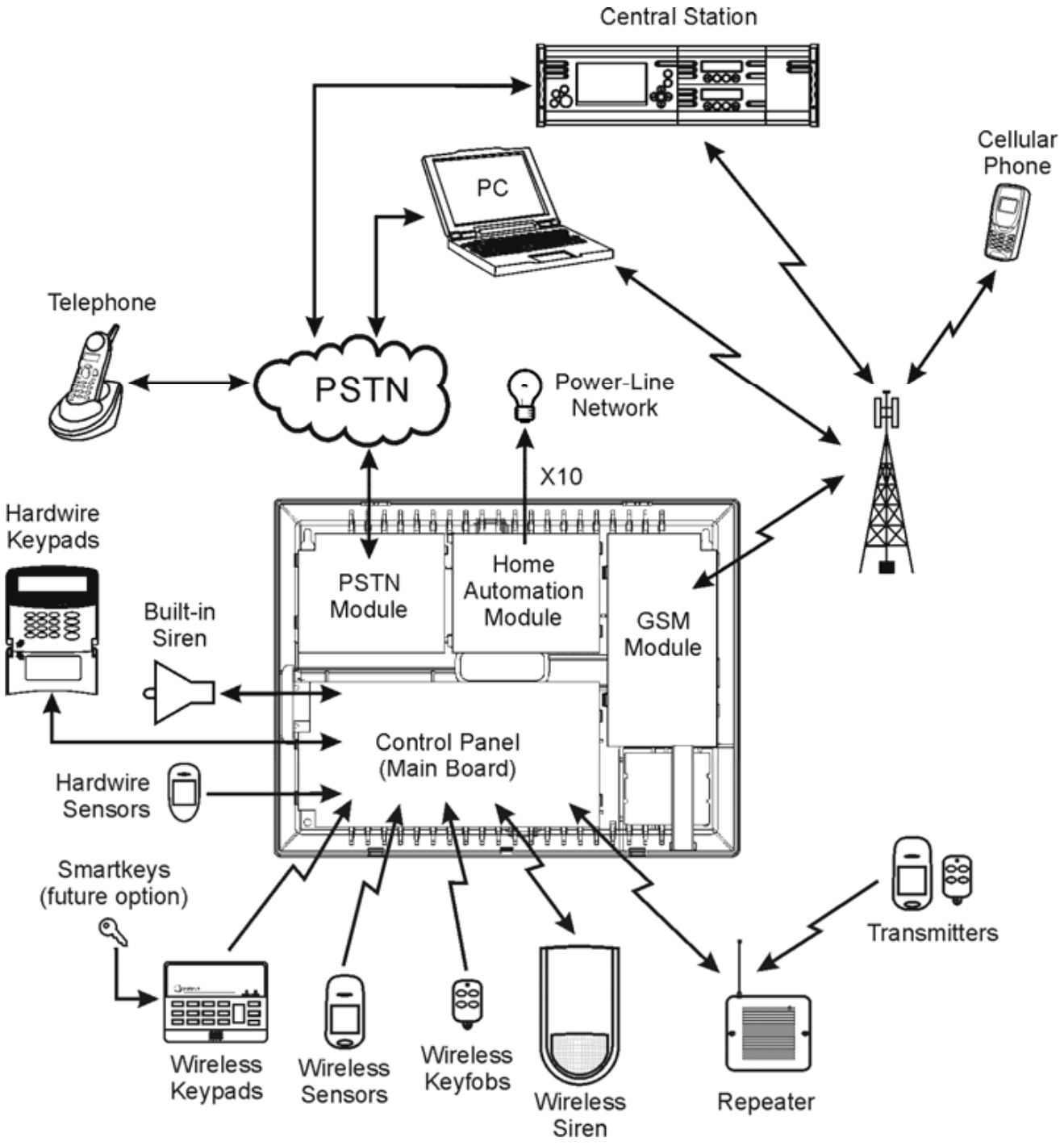


Figure 1.1: System Architecture

© MARMITEK

1.4: Hardware Layout

The aim of this section is to acquaint you with the various circuit boards that make up the system. Apart from the Main Board, each peripheral module is available as an optional extra designed for installation inside the plastic housing.

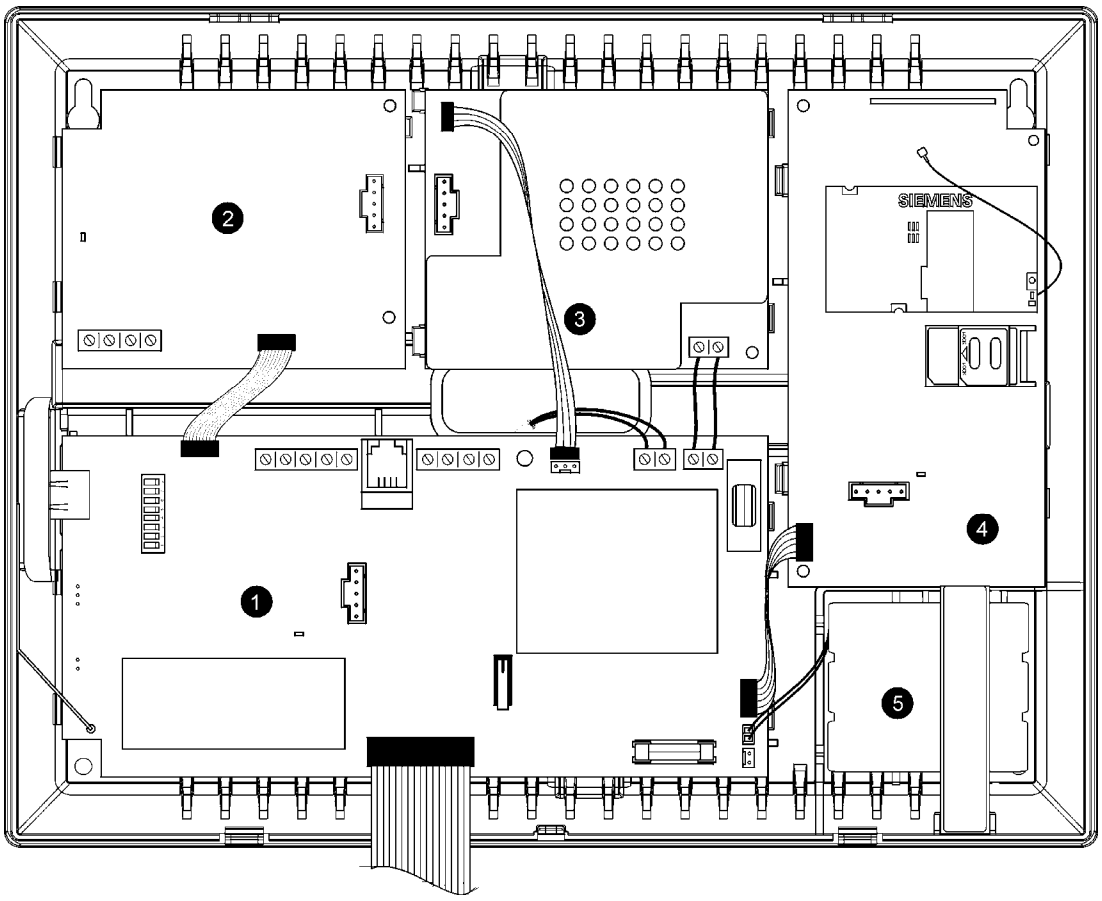


Figure 1.2: System Layout

1. Main Board
2. PSTN dialer module (optional)
3. Home Automation module (optional)
4. Cellular communications module (optional)
5. Backup battery pack

1.4.1: The Main Board

The Main Board is the brain of the system and connects to various peripheral modules using a number of interface connectors. Additionally, the Main Board includes a programmable output, a hardwire zone input and a USB port for PC programming.

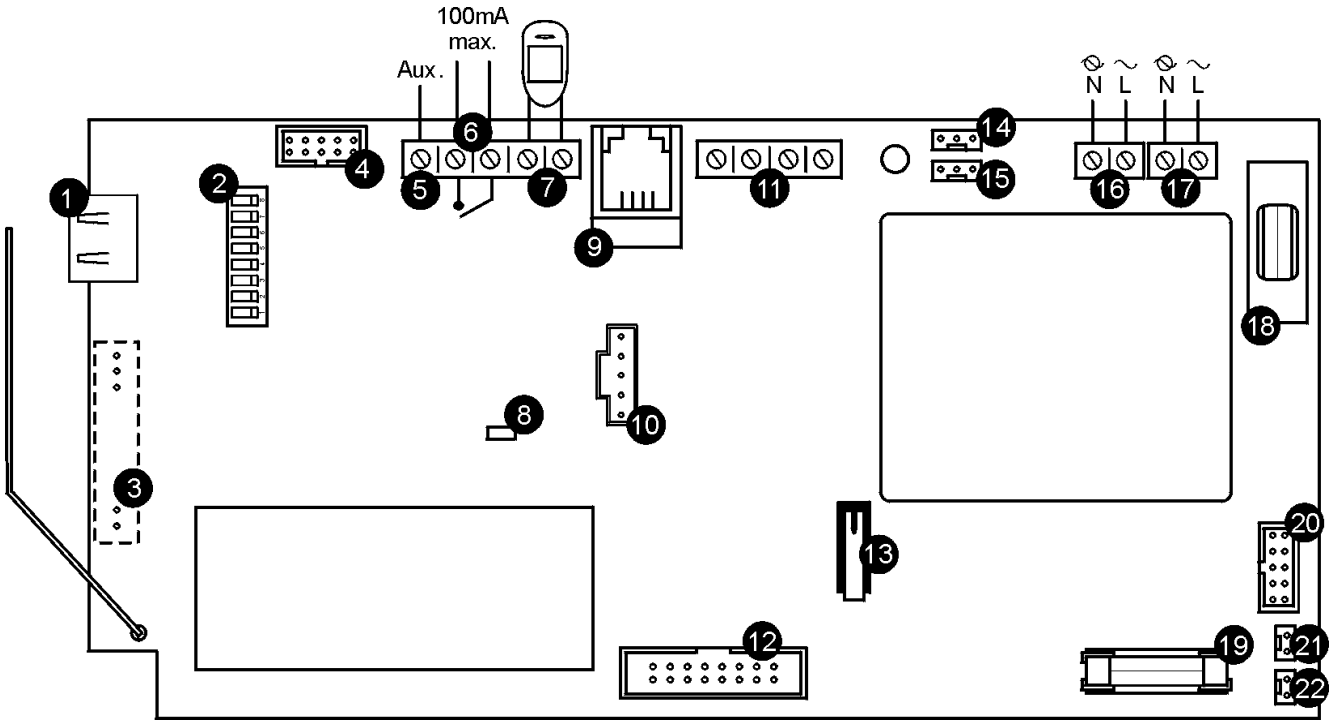


Figure 1.3: Main Board

1. USB port for connection to PC
2. DIP-switch for flash programming
3. Connector for on-board transmitter
4. Flat-cable interface connector to PSTN module
5. Auxiliary power output (AC Operated:10-15V, Battery Operated: 6-8V)
6. Programmable relay output (100mA max. load)
7. Hardwire zone (Zone 33)
8. Status LED
9. Interphone module connector
10. Flash programming connector for main board
11. HK855 Hardwire LCD Keypad terminal block
12. Flat-cable interface connector to LCD keypad, built-in speaker, microphone and siren
13. Front tamper switch
14. Programming keypad connector (optional)
15. Interface connector to Home Automation module
16. AC power terminal block
17. Home Automation module terminal block
18. AC power protection fuse
19. Backup battery protection fuse
20. Flat-cable interface connector to GSM module
21. Backup battery connector
22. Additional backup battery connector

© MARMITEK

1.4.2: PSTN Module

The PSTN module provides the system with a standard dialer for communication via the Public Switched Telephone Network (PSTN).

Do not use VoIP phone lines for communication to the central monitoring station. In certain cases the system may not transmit alarm signals successfully over the VoIP network.

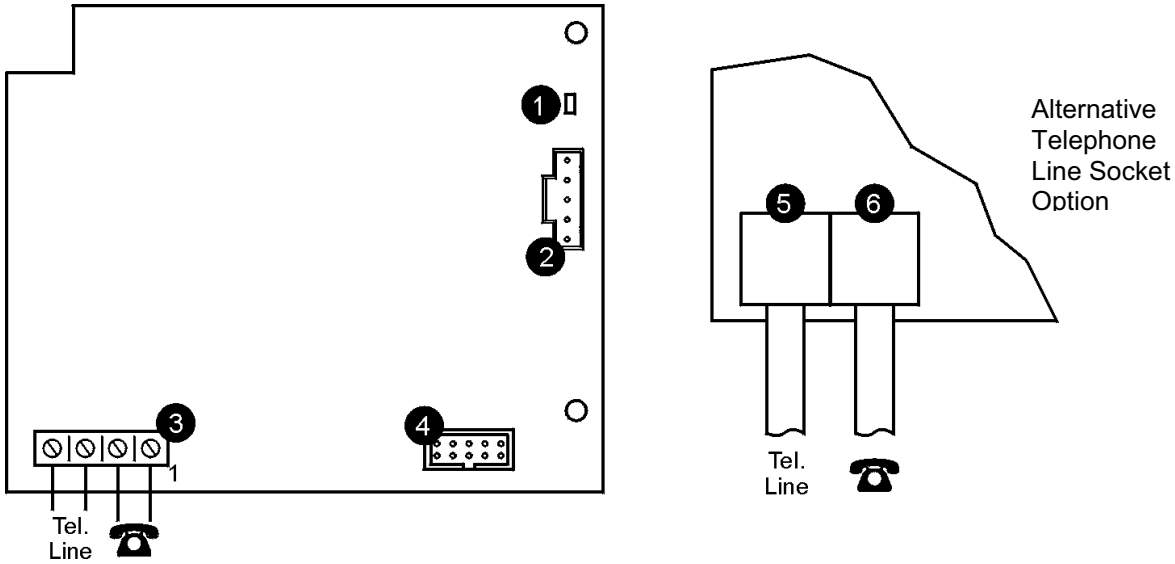


Figure 1.4: PSTN Module

1. Status LED
2. Flash programming connector
3. Telephone line terminal block (Terminals 1 & 2: Incoming line from telephone company, Terminals 3 & 4: Outgoing line to telephone)
4. Flat-cable interface connector to Main Board
5. Telephone socket for incoming line from telephone company
6. Telephone socket for outgoing line to telephone

1.4.3: Home Automation Module

The Home Automation module provides the system with an interface to the power-line network, enabling control over 16 home automation units employing the X-10 protocol.

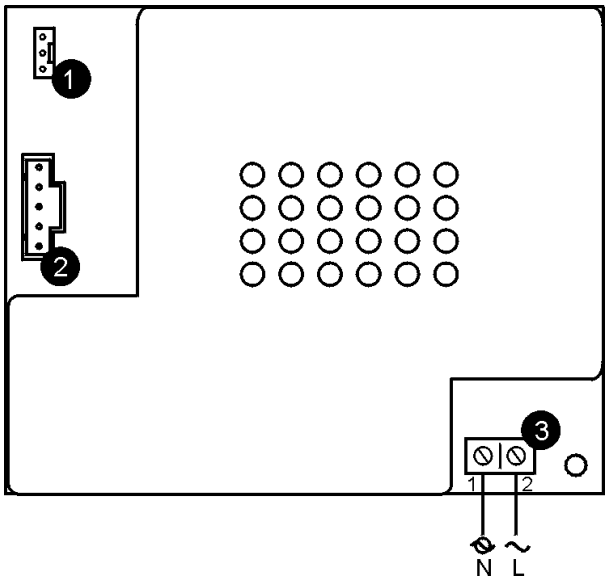


Figure 1.5: Home Automation Module

1. Interface connector to Main Board
2. Flash programming connector
3. Power-line terminal connections to Main Board (**1** - Neutral; **2** - Live)

1.4.4: Cellular Communications Module

The Cellular Communications module enables the control panel to communicate via cellular networks. This offers the ability to send or receive SMS messages, perform up/downloading, implement cellular 2-way voice applications.

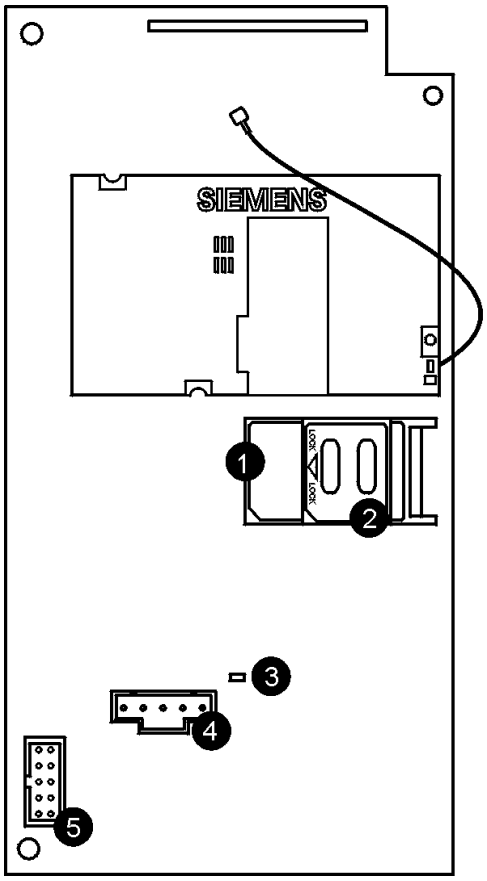


Figure 1.6: Cellular Communications Module

1. SIM card holder
2. SIM card release
3. Status LED
4. Flash programming connector
5. Flat-cable interface connector to Main Board

© MARMITEK

The following chapter explains how to install the system and provides guidelines and tips on how to optimize the installation. It is recommended that you familiarize yourself with the various circuit boards that make up the system – *see 1.4: Hardware Layout*.

2.1: Pre-Installation Planning

Before starting the installation procedure, it is worthwhile to draw a rough sketch of the building and determine the required position for the control panel and each wireless device.

When deciding on the placement for installation, consider the following:

- Mount the control panel in a location with easy access to telephone and power connections.
- If installing with the GSM Cellular Communications module, the control panel should be mounted in a position where the GSM signal is strong.
- Refer to the following section in order to choose the optimal location for wireless devices in relation to the control panel.

2.1.1: Wireless Installation Guidelines

In order to optimize wireless communication, consider the following guidelines:

- Whenever possible, mount the panel centrally in relation to wireless sensors.
- Avoid installation in close proximity to sources of high noise or radio frequency interference. For example, metal air conditioner/heater ducts and circuit breaker boxes.
- Minimize the distance between the panel and transmitters.
- Minimize the number of obstacles between the panel and transmitters.

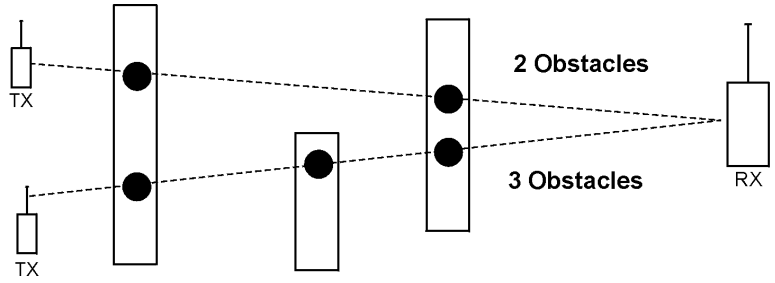


Figure 2.1: Minimizing Obstacles

- Metal based construction materials, such as steel reinforced concrete walls, reduce the range of radio transmissions.

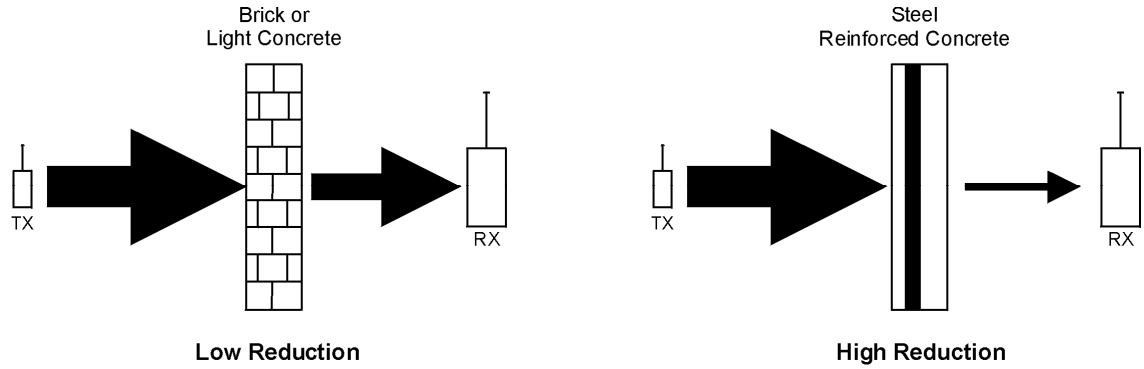


Figure 2.2: Considering Construction Materials

- The reduction of the RF signals' strength is directly proportional to the thickness of the obstacle, assuming that the obstacles are of identical material.

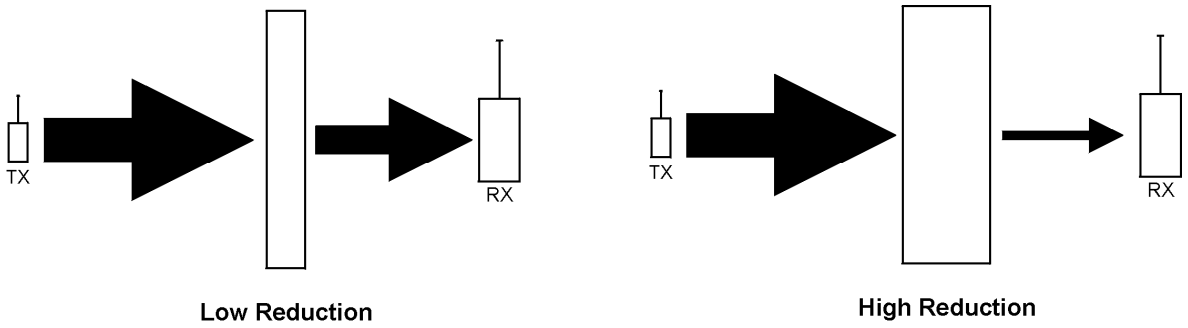


Figure 2.3: Considering Thickness of Obstacles

2.2: Installation Procedure

After unpacking the kit and making certain that you have all the necessary equipment, it is recommended that you install the system as follows:

STEP 1: Open the housing.

STEP 2: Temporarily power up the system.

STEP 3: Register the transmitters.

STEP 4: Test the chosen mounting location.

STEP 5: Permanently install the control panel and transmitters.

2.2.1: Step 1 – Opening the Housing

To open the housing:

1. Remove the housing screw located at the bottom of the front cover.
2. Using a screwdriver carefully press the release tabs as shown in Figure 2.4.
3. Lift the front cover away from the back of the housing. You will notice that the front cover is attached to the back with two fastening bands and the keypad's flat cable.

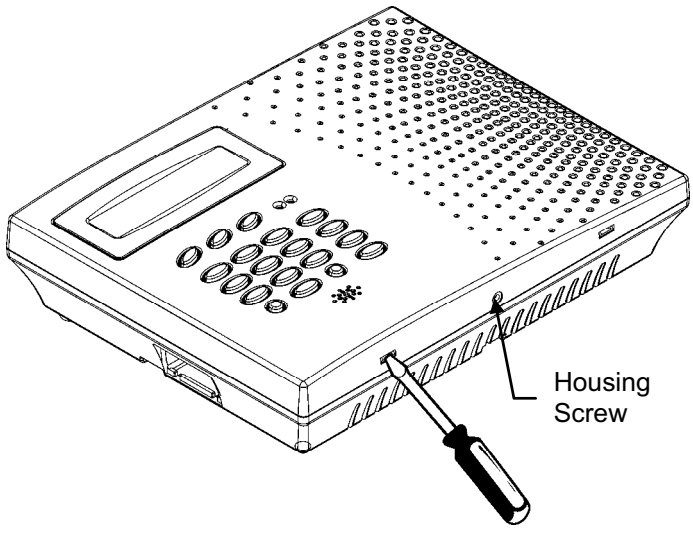


Figure 2.4: Opening the Housing

2.2.2: Step 2 – Powering Up the System

In order to register and test transmitters, it is necessary to temporarily power up the system before installing the control panel. At this stage, do not connect the backup battery.

Thread the power cable through the wiring hole on the back cover and connect the cable to the AC power input on the Main board. For the exact location of the AC power input, see section *1.4.1: The Main Board*. Close the front cover and apply AC power. At this stage, ignore any trouble conditions that may appear on the LCD display (e.g. Low Battery).

© MARMITEK

2.2.3: Step 3 – Registering Transmitters

For the control panel to recognize a device, its transmitter must be registered. In general terms, transmitter registration means sending two transmissions from a device when the control panel is in "Registration" mode.

To register a device:

1. Press ✓.
2. Enter your Installer code (the default Installer code is **1111**).
3. Enter **91** (Programming, Devices) to enter the Devices menu.
4. Press the menu navigation keys (▲/▼), until the type of device you want to register appears on the LCD display (e.g. Zones or Keypads).
5. Press ✓.
6. Press the menu navigation keys (▲/▼), until the exact device you want to register appears on the LCD display (e.g. Zone 3 or Keypad 2).
7. Press ✓. If a device has not been registered at the chosen location, the control panel initiates Registration mode. During Registration mode, the system waits for two transmissions from the device.

If a device has already been registered at the required location, the system will not initiate Registration mode. If the device has already been registered at another location, attempts to register are ignored by the system.

8. Send two transmissions from the device – *refer to each device's installation instructions in Appendix B for further details.*
9. When ***Save?*** is displayed on the control panel's LCD, press ✓. The display automatically switches to the next option for that device. For example, pressing ✓ to confirm Zone registration automatically moves you to the Zone Type option.
10. Continue entering other parameters for the chosen device.

Pressing × returns you to the previous menu level. Press ×when you are in the Main menu (Menu Level 1) to exit menu mode.

2.2.4: Step 4 – Testing the Chosen Mounting Location

Once all of the transmitters are registered, it is recommended that you test the chosen mounting locations before permanently mounting the control panel and wireless devices. You can test the transmitter signal strength using the TX Test feature.

To test transmitter signal strength.

1. Press ✓.
2. Enter your Installer code.
3. Enter **7072** (Service, Transmitters, TX Test) to initiate TX Test mode.
4. Activate the transmitter you wish to test; the transmitter's details appear on the control panel's LCD. Additionally, between one and four tones are sounded to indicate the transmitter's signal strength. If four tones are sounded, the transmitter is in the best possible location – *see 4.7.7: Transmitters* for further information.
5. After you have tested each transmitter, press × to exit TX Test mode.

If installing with the GSM Cellular Communications module, test the GSM signal strength using the system's RSSI meter.

To test the GSM signal strength:

1. Press ✓.
2. Enter your Installer code.

3. Enter **709** (Service, GSM Signal); the signal strength of the cellular network is displayed – *see 4.7.9: GSM Signal Strength* for further information.

2.2.5: Step 5 – Installing the Control Panel and Transmitters

Having chosen and tested the mounting location of the control panel and each transmitter, you are now ready to permanently install the system.

To permanently install the transmitters, refer to each device's installation instructions (in Appendix B of this manual or supplied individually with each product).

To install the control panel:

1. Disconnect AC power from the control panel.
2. Open the housing as explained in section 2.2.1: Step 1 – Opening the Housing.
3. Remove the backup battery pack. If you want to install the control panel with back tamper, it is also necessary to disconnect the flat cable connecting the Main board to the front panel keypad and remove the Main board. Figure 2.5 shows the control panel with the Main board and the battery pack removed.

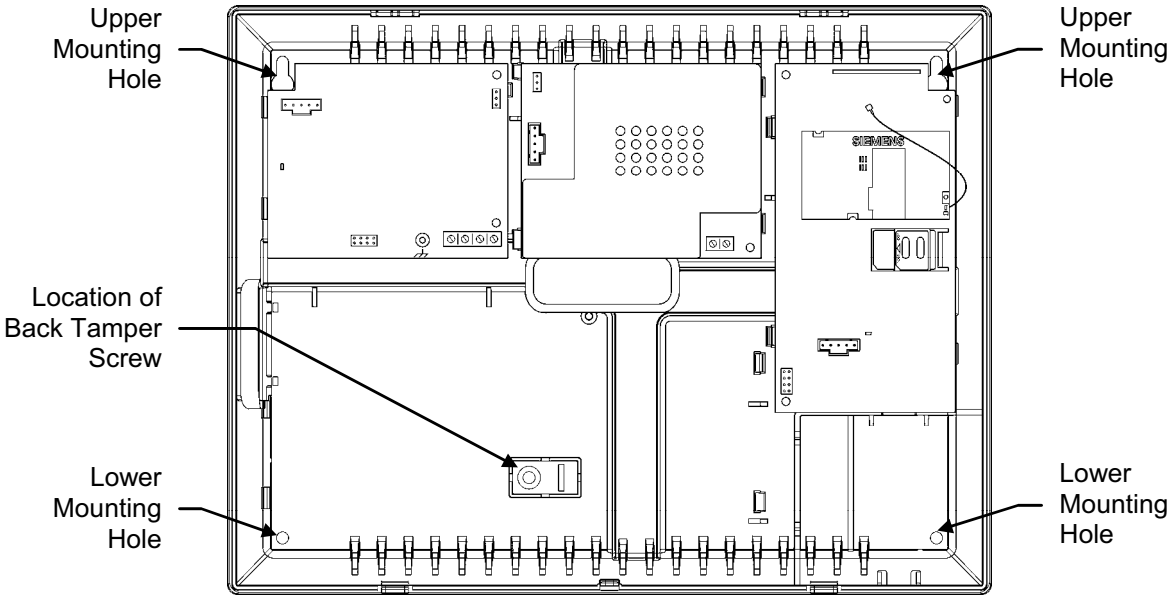


Figure 2.5: Back Cover (Main Board and Battery Pack removed)

4. Place the control panel in position against the wall and mark the upper and lower mounting holes. If using the back tamper, also mark the hole for the back tamper screw.
5. Install wall anchors in the appropriate positions.
6. Thread any required cables through the wiring hole on the back cover (e.g. AC power and telephone line) and make any necessary wiring connections.
7. Connect the power cable to the AC power input on the Main board – *see 1.4.1: The Main Board*.
8. Connect the telephone line to the Telephone Line terminal block on the PSTN module – *see 1.4.2: PSTN Module*.
9. Connect any additional HK855 Hardwire LCD Keypads if required – *see 2.4: Installing HK855 Hardwire LCD Keypads.*

© MARMITEK

10. Mount the control panel to the wall using four screws and insert the back tamper screw if required – *see 2.3: Back Tamper*.

The control panel shall be mounted so that it shall withstand a force of at least three times its own weight.

11. Replace the Main Board and reconnect its peripheral modules.
12. Connect the flat cable connecting the Main board to the front panel keypad and the replace the front cover's fastening bands.
13. Apply AC power.

Always connect AC power before connecting the battery pack. Batteries are supplied uncharged. When you first connect the battery, it is probable that the system will display a Low Battery condition. Allow the battery to charge for at least 18 hours before use.

14. Connect the battery pack to the connector on the Main Board.
15. Position the front cover's top holding hooks onto the back cover and snap the front cover closed.
16. After installing the control panel, perform the Find Modules function – *see 12.5: Find Modules.*

2.3: Back Tamper

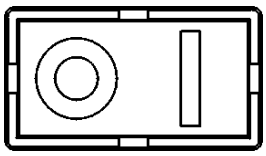


Figure 2.6: Perforated Back Tamper Release

The back tamper switch is an optional feature that provides an extra safeguard in the event that the control panel is removed from the wall.

The back tamper switch is located on the rear side of the control panel's Main Board and is constantly depressed by the section of the back cover shown in Figure 2.6.

For this feature to operate, you must insert a screw into the back tamper mounting hole – *see section 2.2.5: Step 5 – Installing the Control Panel and Transmitters.* When the control panel is removed from the wall, the screw causes the perforated section of the plastic to break and remain attached to the wall. As a result, the back tamper switch is released and an alarm is generated.

2.4: Installing HK855 Hardwire LCD Keypads

The system supports HK855 Hardwire LCD Keypads that may be installed up to 300m from the control panel.

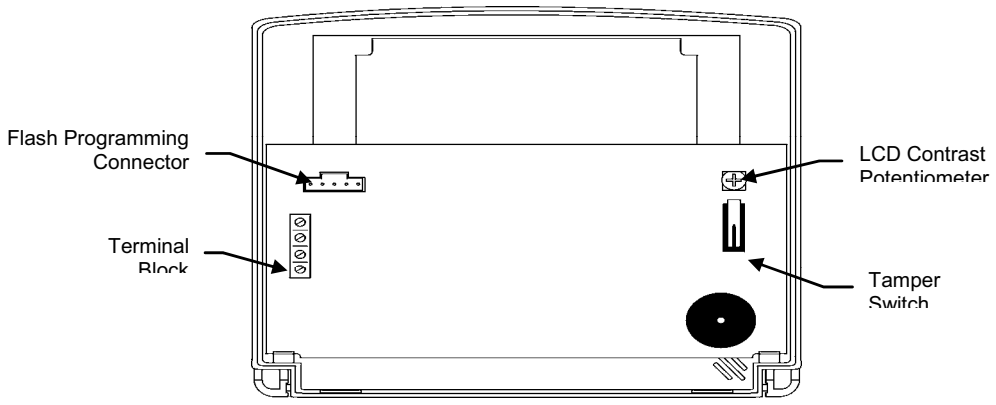


Figure 2.7: HK855 Hardwire LCD Keypad (back cover off)

To install HK855 Hardwire LCD Keypads.

1. Disconnect all power, both AC and battery, from the control panel.
2. Remove the back cover of the keypad. To do so, press the two snaps (located at the bottom of the keypad) using a small flat-head screwdriver and carefully pull the back cover away from the front of the housing.
3. Place the back cover of the keypad in position against the wall and mark the upper and lower mounting holes.
4. Install wall anchors in the appropriate positions.
5. Thread the cable from the control panel through the wiring hole on the back cover and attach the back cover to the wall using four screws.
6. Connect the terminal block on the keypad to the appropriate terminal block on the control panel's main board as shown in Figure 2.8.

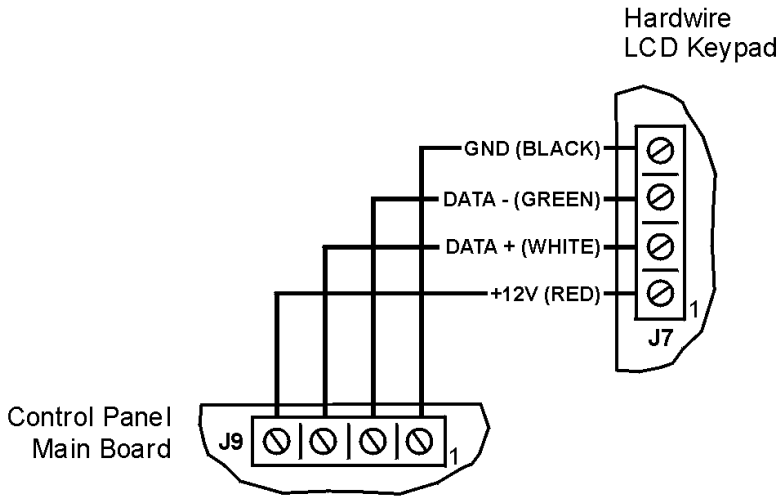


Figure 2.8: Connections for HK855 Hardwire LCD Keypad

7. Reapply power to the control panel.
8. Set the keypad address as follows:
    a. Make certain the keypad's tamper switch is open.
    b. On the keypad, press keys 1, 3 and 5 simultaneously.
    c. Use the arrow keys (▲/▼) to select the keypad address.
    d. Press ✓.
9. Position the front cover's top holding hooks onto the back cover and snap the front cover closed.
10. After installing hardwire keypads, perform the Find Modules function – *see 12.5: Find Modules.*

© MARMITEK

3.1: Front Panel Layout

The front panel provides a detailed interface for operating and programming the system. The following diagram will familiarize you with the various elements on the front panel.

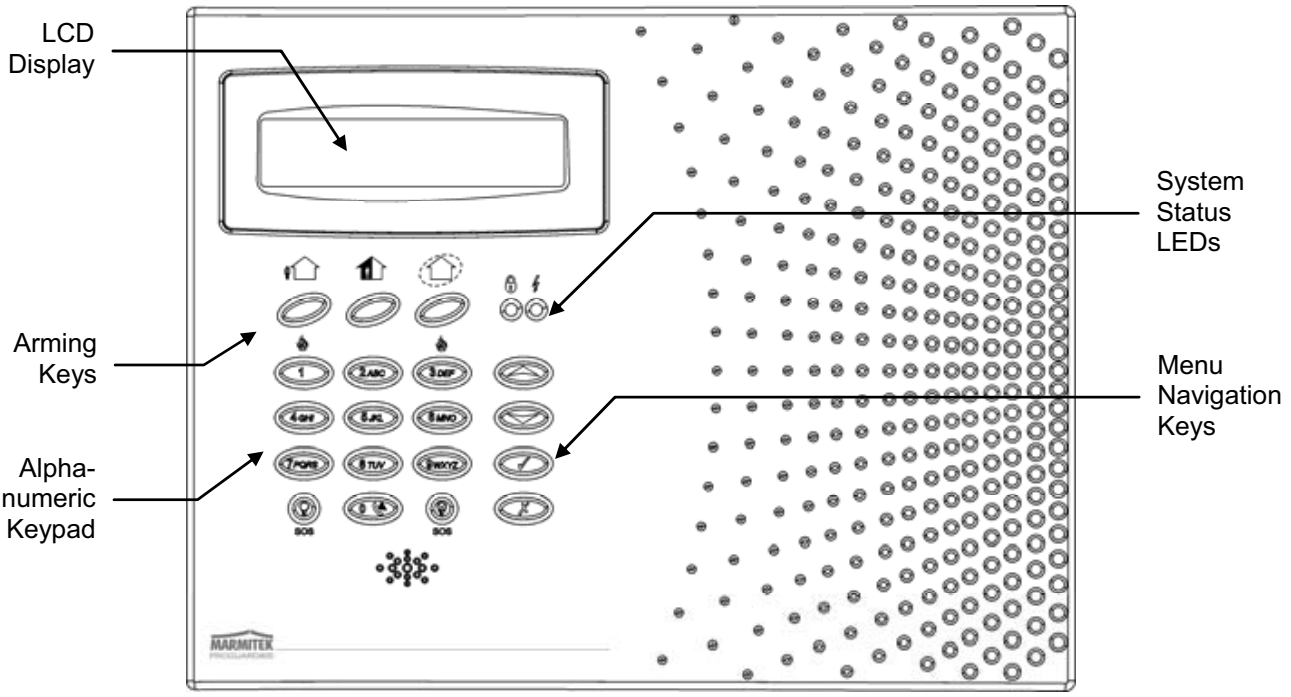


Figure 3.1: Front Panel

3.2: System Status LEDs

The two LEDs, Armed and Power, provide essential information on the status of the system.

If the Armed LED is…	It means…
Off	The system is disarmed.
On	The system is armed.
Flashing	An alarm has occurred. Alarm indication is cleared the next time that an arming sequence is initiated or after the relevant event has been viewed in the event log.

Table 3.1: Armed LED Indication

Alarm indication is not displayed after a silent panic alarm.

If the Power LED is…	It means…
Off	Both AC and Battery power are disconnected.
On	System Power is OK.
Flashing (slow)	Backup battery low or low battery from transmitters.
Flashing (fast)	AC loss.

Table 3.2: Power LED Indication

3.3: Front Panel Keypad

The alphanumeric keypad on the front panel enables you to perform various operation and programming tasks. Apart from the regular functions of a standard alphanumeric keypad, the keypad offers a number of special functions. These functions are listed in the following table.

Key	Special function
1	Used to enter symbols in descriptor editing.
0	Used to enter symbols in descriptor editing.
×	Used to cancel the current selection. Used to return to the previous menu level.
✓	Used to enter Menu mode. Used to select the current menu item. Used to signify the end of an entered value. Toggles status in Zone Bypass/Unbypass function.
💡	Used to switch Home Automation units on. In descriptor editing, used to insert a space before the current character. In phone number editing, used to enter “T”, “,”, “P”, “+”, “*”, “#”. In account number editing, used to enter Hexadecimal digits (A-F). Toggles item descriptors and default names. In the event log, toggles the time/date stamp. Toggles AM and PM when setting the time in 12hr format.
⊗	Used to switch Home Automation units off. In descriptor and phone number editing, used to delete the current character.
▲	Used to scroll backwards in the current menu level. For Global Chime and Message Center features, used to access shortcuts. ▲ + ▼ (Global Chime shortcut) ▲ + × (Record Message shortcut) ▲ + ✓ (Play Message shortcut)
▼	Used to scroll forwards in the current menu level. During standby, used to scroll through the list of system trouble conditions.

Table 3.3: Front Panel Keypad Functions

3.4: LCD Display

The LCD display provides you with a detailed interface for operation and programming.

3.4.1: Standby Mode

Standby mode can be defined as the state the system is in when it is disarmed and not in Menu mode. In Standby mode, the armed status, system status or banner are displayed. If system status is normal, the current time is displayed.

Figure 3.2: Typical Standby Display

© MARMITEK

This…	Means…
DISARMED	The system is disarmed.
FULL ARMED	The system has been armed using the displayed arming method.
PART ARMED	
PERIMETER ARMED	
FULL ARMING	The system is in the process of arming (displayed during exit delay).
PART ARMING	
PERIMETER ARMING	
PART ARMED INST	The system has been armed using the displayed arming method with the Instant arm feature activated.
PERIM ARMED INST	
PART ARMING INST	The system is in the process of arming with the Instant arm feature activated.
PERI ARMING INST	

Table 3.4: Armed Status

This…	Means…
ZONES IN ALARM	Zones have been violated.
TAMPER ALARM	The system has been tampered with.
56 TO EXIT	The exit delay is counting down (56 seconds remaining).
11 TO DISARM	The entry delay is counting down (11 seconds remaining).
SYSTEM NOT READY	The system is not ready to arm, check that all doors and windows are closed.
KEYPAD LOCKED	Five unsuccessful attempts were made to enter a user code, the keypad is locked for 30 minutes.
SYSTEM TROUBLE	A trouble condition has been detected, press ▼ for further details.

Table 3.5: System Status

3.4.2: System Trouble Tones

In the event of system trouble, the *ProGuard800* sounds a series of tones to alert the user. To silence these tones, press ▼ and scroll through the system trouble list displayed on the LCD. When the trouble condition is restored, it is removed from the system trouble list.

For this feature to function, Trouble Tones must be enabled in programming – see 8.8.1: Trouble Tones.

System trouble tones are not sounded from 10:00pm to 7:00am so as not to disturb household members who may be asleep. However, you can program the system to immediately annunciate telephone trouble at all times – *see 8.8.2: Telephone Trouble Tones.*

3.5: Vocal Message Annunciation

Certain versions of the *ProGuard800* hardware, support vocal annunciation of system status. If this feature is enabled in programming (see 9.13: Vocal Messages), the system plays short messages to indicate arming, disarming, bypassed zones, system trouble, water alarm and message waiting.

The availability of the Vocal Message annunciation feature is hardware dependent.

3.6: HK855 Hardwire LCD Keypad

In addition to the front panel keypad, you can install up to three, individually addressed, HK855 Hardwire LCD Keypads (or two keypads with large LCD). The layout of the HK855 Hardwire LCD Keypad is similar to the front panel keypad and most of the functionality is identical. The following diagram shows the layout of the HK855 Keypad.

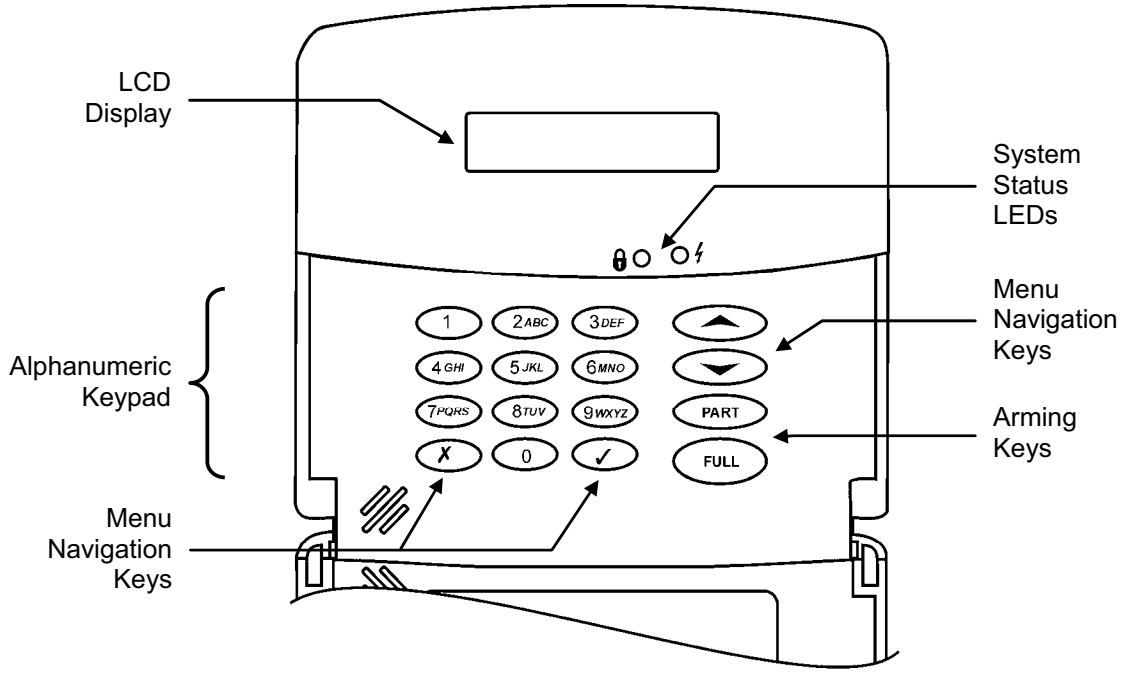


Figure 3.3: HK855 Hardwire LCD Keypad (PROGUARD800-KPD/S)

As with the front panel keypad, the HK855 Hardwire LCD Keypad also provides a number of special functions that are listed in the following table.

Key	Special function
1	Used to enter symbols in descriptor editing.
0	Used to enter symbols in descriptor editing.
×	Used to cancel the current selection. Used to return to the previous menu level.
✓	Used to enter Menu mode. Used to select the current menu item. Used to signify the end of an entered value. Toggles status in Zone Bypass/Unbypass function.
FULL	Used to arm the system fully. In descriptor editing, used to insert a space before the current character. In phone number editing, used to enter “T”, “,”, “P”, “+”, “*”, “#”. In account number editing, used to enter Hexadecimal digits (A-F). Toggles item descriptors and default names. In the event log, toggles the time/date stamp. Toggles AM and PM when setting the time in 12hr format.
PART	Used to arm the system partially (Part or Perimeter). In descriptor and phone number editing, used to delete the current character.
▲	Used to scroll backwards in the current menu level. Used to access the Global Chime shortcut (▲ + ▼).
▼	Used to scroll forwards in the current menu level. During standby, used to scroll through the list of system trouble conditions.

Table 3.6: HK855 Hardwire LCD Keypad Special Functions

© MARMITEK

3.7: Arming/Disarming

The following section explains how to arm and disarm the control panel using the LCD keypad.

The *ProGuard800* offers three arming modes that you can define to suit the application. Figure 3.4 illustrates the three arming modes. In each diagram, the protected area is shaded.

Figure 3.4: Arming Modes

The arming options are entirely flexible. You can program each sensor to be included in any combination of the three arming modes – *see section 7.6.2: Arm Set.* Additionally, each arming mode has a separate exit and entry delay.

The arming functions are only available while the system is in Standby mode.

3.7.1: Arming Keys

The Arming keys enable you to arm the system using any of the three arming methods: Full, Part and Perimeter.

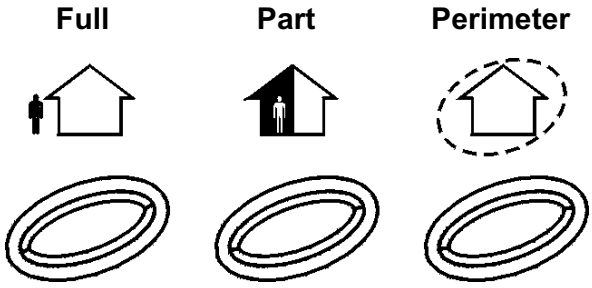


Figure 3.5: Arming Keys

3.7.2: Full Arming

Full arming is designed for when the occupant vacates the premises.

To fully arm the system:

1. Check if the system is ready to arm.
2. Press the Full arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code. *See 9.3.2: One-Key Arming*

3.7.3: Part Arming

Part arming is designed for when the occupant intends to remain inside one part of the premises and secure another part.

To partially arm the system using the front panel keypad:

1. Check if the system is ready to arm.
2. Press the Part arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code.

To partially arm the system using the HK855 Hardwire LCD Keypad:

1. Check if the system is ready to arm.
2. Press PART on the keypad.
3. Select Part arming.
4. If One-Key Arming is disabled, enter your user code.

3.7.4: Perimeter Arming

Perimeter arming is designed for when the occupant intends to remain inside the premises and secure the perimeter.

To arm the system's perimeter using the front panel keypad:

1. Check if the system is ready to arm.
2. Press the Perimeter arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code.

To arm the system's perimeter using the HK855 Hardwire LCD Keypad:

1. Check if the system is ready to arm.
2. Press PART on the keypad
3. Select Perimeter arming.
4. If One-Key Arming is disabled, enter your user code.

3.7.5: Combination Arming

The system allows you to activate a combination of two arming modes. If you Perimeter arm the system, you may also activate Full or Part arming. Likewise, you can Perimeter arm the system after activating Full or Part arming. It is not important which arming mode you choose first.

You can activate the second arming mode during the exit delay of the first arming mode. If the first exit delay expires, you cannot activate a second arming mode.

To arm the system using two arming modes:

1. Check if the system is ready to arm.
2. Activate the first arming mode.
3. If One-Key Arming is disabled, enter your user code.
4. While the exit delay of the first arming mode is counting down, activate the second arming mode.
5. If One-Key Arming is disabled, enter your user code.

It is not possible to activate Full and Part arming modes simultaneously.
It is necessary to disarm first when changing from one arming mode to another arming mode.

The exit delays of the two arming modes are entirely independent. The moment an arming mode is activated, its exit delay begins to count down. The entry delay depends on which sensor was tripped first. For example, if the sensor is included in Full arming, the entry delay for Full arming counts down – *see 7.6.2: Arm Set*. If the sensor is included in both activated arming modes, the entry delay for Perimeter arming counts down.

If, due to open zones, the system is not ready to activate the second arming mode then both arming methods are cancelled. In this case, check that the relevant entrances are secured and start the entire arming sequence again.

© MARMITEK

Disarming cancels both active arming modes.

3.7.6: Forced Arming

Forced arming enables you to arm the system when the system is not ready. For example, if a door protected by a magnetic contact is open, you may arm the system on condition that the door will be closed by the end of the Exit delay. If the door is still open after the exit delay expires, an alarm is generated.

Two conditions enable you to perform Forced arming:

- Forced arming is enabled – *see section 9.3.1: Forced Arm.*
- The sensor that is causing the System Not Ready condition is Force Arm enabled – *see section 7.6.5: Force Arm.*

3.7.7: Instant Arming

Instant arming is a feature that allows you to cancel the entry delay after Part or Perimeter arming the system. For this feature to function, it must be enabled in programming – *see 9.3.4: Instant Arm*.

To instantly arm the system.

1. Check if the system is ready to arm.
2. Press the Part or Perimeter arming key on the keypad and enter your user code if One-Key Arming is disabled.
3. Press and hold down ▲ on your keypad until the message ***Instant Arming, OK?*** is displayed
4. Press ✓; the exit delay for the current arming period is cancelled.

3.7.8: Disarming

When a sensor is tripped, the entry delay counts down; each arming method has its own entry delay.

To disarm the system:

- Enter a valid user code.

If the Cancel Alarm feature is enabled (see 9.18: Cancel Alarm), disarming the system within five minutes of an alarm causes the control panel to send an Alarm Cancelled event to the monitoring station. In this case, a message is displayed on the keypads' LCD and the control panel does not allow any local function to be performed until ✓ is pressed for confirmation.

3.8: Remote Arming/Disarming via SMS

You can arm and disarm the system remotely by sending the SMS commands from a cellular phone to the cellular communications module. Additionally, you can check the arm status of the system by sending an Arm Status request message.

Each SMS command contains the following elements:

❶ SMS Command Descriptor (up to 43 characters of free text)
❷ # (delimiter – separates the descriptor from the actual command)
❸ User Code (4 digits)
❹ Command (120=Disarm, 121=Full Arm, 122=Part Arm, 123=Perimeter Arm, 124=Full + Perimeter Arm, 125=Part + Perimeter Arm, 200 = Arm Status)

The following example shows the format of an SMS command for arming the system:

❶								❷	❸				❹		
F	u	L	l		A	r	m	#	1	2	3	4	1	2	1

While the SMS Command Descriptor is optional, you must start the SMS command with the # symbol for the system to accept the command.

After an SMS command is executed by the system, you can program the system to return a confirmation message to the sender – *see 10.7.5: SMS Confirmation.*

3.8.1: Arm Status Reply

On receiving an Arm Status request message, the system returns a status message to the sender. This message includes the system status and the descriptor of the user or the device used to arm/disarm the system.

The following example shows an Arm Status reply where the system has been fully armed by a user named Mark.

F	U	L	L		A	R	M	E	D	-	M	A	R	K

3.9: Remote Arming/Disarming via DTMF

Using the Telecontrol feature, you can fully arm and disarm the system via the telephone with DTMF commands. For further information on the Telecontrol features, see Chapter Five: Telecontrol and 5.1.5: Arm/Disarm DTMF Commands.

3.10: LCD Keypad Alarm Activation

In the event of an emergency, the user can generate three kinds of alarm from the front panel keypad and the HK855 Hardwire LCD Keypads.

To activate an SOS alarm from the front panel keypad:

- Press both Home Automation keys simultaneously.

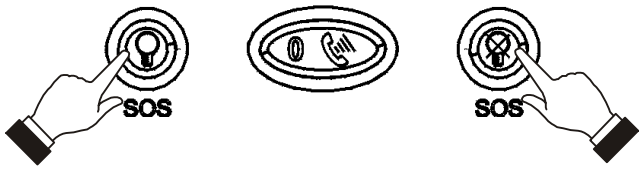


Figure 3.6: SOS Alarm Activation (front panel keypad)

To activate an SOS alarm from the HK855 Hardwire LCD Keypad:

- Press × and ✓ simultaneously.

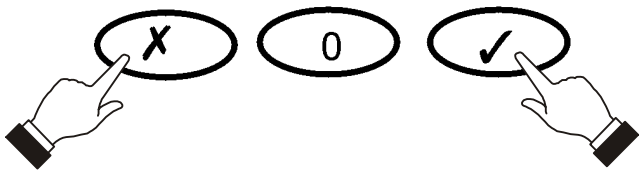


Figure 3.7: SOS Alarm Activation (HK855 Hardwire LCD Keypad)

To activate a Fire alarm from the front panel or HK855 Hardwire LCD Keypad:

- Press keys 1 and 3 simultaneously.

© MARMITEK

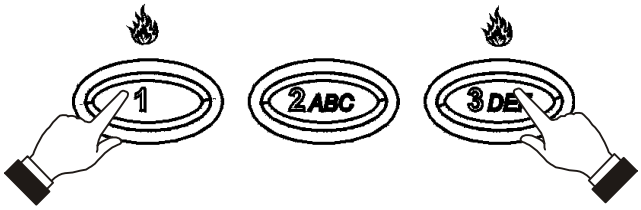


Figure 3.8: Fire Alarm Activation

To activate a Medical alarm from the front panel or HK855 Hardwire LCD Keypad:

- Press keys 4 and 6 simultaneously.

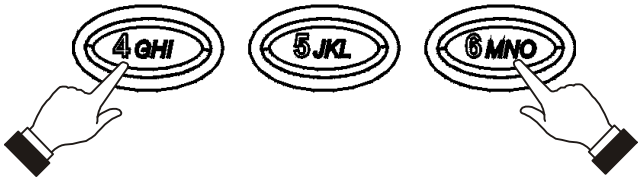


Figure 3.9: Medical Alarm Activation

Chapter Four: Advanced System Operation

Besides the basic arming functions described in the previous chapter, you can access additional functions via the menu. This chapter describes these functions and the menu navigation procedure.

4.1: Menu Navigation

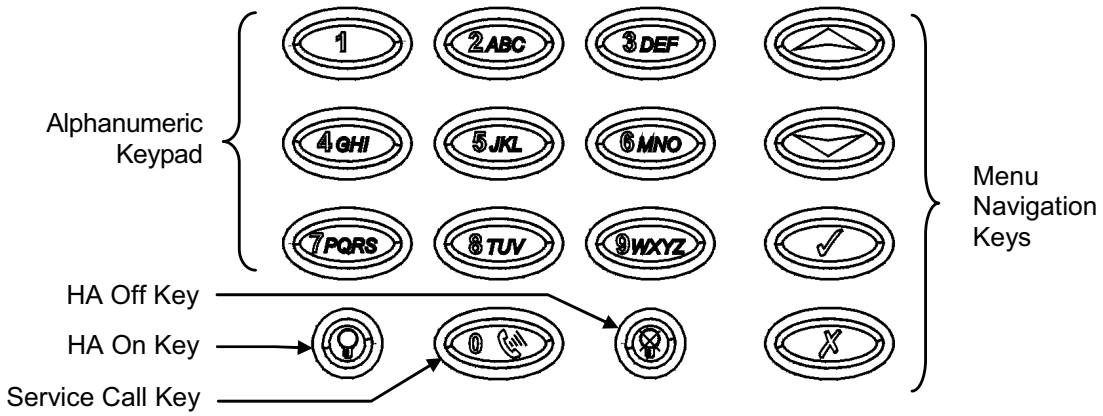


Figure 4.1: On-board Keypad Layout

The LCD keypad's friendly, menu-driven interface is designed to facilitate operation and provide a gentler learning curve for first-time users. You can navigate through the menus using the arrow navigation keys (▲/▼) and make simple yes/no decisions using the ✓and × keys.

For example, perform the following procedure to navigate to Service, Interface Test.

1. Press ✓ to enter Menu mode.
2. Enter an authorized user code; the first menu item, ***1. Stop Comm.***, is displayed.
3. Press ▼ until ***7. Service*** is displayed.
4. Press ✓ to enter the Service menu.
5. Press ▼ until ***5. Interface Test*** is displayed.
6. Press ✓ to choose the displayed function.

As an alternative to scrolling through menu options, you may enter a function's shortcut once you have entered Menu mode. Shortcut numbers appear in square brackets in the procedures throughout this manual.

Press the × key to return to the previous menu level. Press this key when you are in the main menu to exit Menu mode.

4.1.1: Menu Mode Timeout

Menu mode automatically terminates a certain amount of time after the last keystroke. The duration of this timeout depends upon which code is used to enter the menu. Usually the Menu Mode Timeout is two minutes but if you enter menu mode using the Installer code, the timeout is extended to fifteen minutes.

4.2: Stop Communications

To stop communications:

- From the main menu, select Stop Com. [1]; all communication buffers are cleared and all pending messages are cancelled.

© MARMITEK

4.3: Sensor Bypassing/Unbypassing

When a sensor is bypassed, it is ignored by the system and does not generate an alarm when triggered.

To bypass or unbypass a sensor:

1. From the Bypass Zones menu, select Bypass/Unbyp. [21].
2. Using the arrow keys, scroll to the sensor you want to bypass or unbypass.
3. Press ✓ to change the bypass status.
4. Press ×; ***Save Changes?*** is displayed.
5. Press ✓ to confirm the changed bypass status.

To unbypass all sensors:

1. From the Bypass Zones menu, select Unbypass All [22].
2. Press ✓; all sensors are unbypassed

All bypassed zones are automatically unbypassed when the system is disarmed. A fire zone cannot be bypassed.

4.4: User Codes

The control panel supports up to 32 individual user codes. Each of these codes is four digits long. Most system operations require you to enter a valid user code. The ability to perform an operation is defined by your user code's authorization level. These authorization levels are pre-defined for each code as explained below.

Code 1: Master Code

The Master code is the highest user authorization level. With the Master code, you can edit all other user codes except the Installer code, the Guard code and the Monitoring station TWA Code. Additionally, the Master code grants access to the Event Log, the Service menu and Home Automation Schedule programming. The Master code is a "controlled" code. Arming and disarming using this code causes the panel to notify the monitoring station with an Arm/Disarm event message*.

The default Master code is 1234. Change this code immediately after installing the system!

Codes 2-19: Controlled Codes

When you use a controlled user code for arming and disarming, the panel notifies the monitoring station with an Arm/Disarm event message.

Codes 20-25: Non-controlled Codes

Non-controlled codes do not cause the panel to send Arm/Disarm event messages to the monitoring station. The panel sends a Disarm message only if you use this code to disarm the system after an alarm occurrence.

Codes 26-27: Limited Codes

A Limited code enables the user to issue a code that is valid for one day only. This code automatically expires 24 hours after it has been programmed. These codes are "controlled" in that their use for Arm/Disarm is notified to the monitoring station.

* Only if arm/disarm reporting is enabled during System Programming

Code 28: Duress Code

The Duress code is designed for situations where the user is being forced to operate the system. This user code grants access to the selected operation, while sending a Duress event message to the monitoring station.

Code 29: Telecontrol Code

The Telecontrol code is designed to enable the user to perform a number of tasks via their telephone using DTMF commands. Using this code, the user can call their system to arm and disarm, control HA Units, cancel siren activation or establish Two-Way Audio communication.

Code 30: Monitoring station TWA Code

The Monitoring station TWA code is designed to enable the monitoring station operator to establish Two-Way Audio communication with the control panel after an alarm. This code is valid for use for the first ten minutes after an alarm has occurred. This code can only be used for this specific purpose and does not grant access to any additional system functions such as disarming.

Code 31: Guard Code (for future use)

The Guard Code is a future option that is not available in the current firmware.

Code 32: Installer Code

The Installer code grants access to the Programming menu and the Service menu. Additionally, this code enables you to view and clear the Event Log.

The default Installer code is 1111. Change this code immediately after installing the system!

4.4.1: Editing User Codes

To edit a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to edit.
3. From the code's sub-menu, select Edit Code [#1]; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Edit the code.
5. Press ✓; the new code is stored in the memory.

If you enter a code that is identical to an existing user code, the panel sounds an error tone and the new code is not accepted.

Codes 1-29 can be edited only by the Master code. The Installer code, Guard Code and the Monitoring station TWA Code can be edited only by the installer.

4.4.2: Deleting User Codes

To delete a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to delete.
3. From the code's sub-menu, select Edit Code [#1]; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Enter 0000.
5. Press ✓; the code is deleted.

The Installer and Master codes cannot be deleted.

© MARMITEK

4.4.3: User Code Descriptors

Each user code can be assigned a 16-character descriptor. These descriptors help to identify users in the event log and in SMS Follow Me messages.

To edit a code descriptor:

1. From the main menu, select User Codes [4].
2. Select a code.
3. From the code's sub-menu, select Descriptor [#2].
4. Edit the descriptor using the alphanumeric keypad.
5. Press ✓ when you have finished editing.

4.5: Follow Me

The Follow Me feature is designed to notify the user that certain events have occurred. The events that are sent to the Follow Me telephone number are those events that the user is authorized to view in the event log; events that can be viewed only by the installer are not sent to the Follow Me number – *see Appendix C: Event Table*. If using the TWA Follow Me feature, the audio channel is opened after alarm events only.

To edit the Follow Me number:

1. From the main menu, select Follow Me [5].
2. Enter a telephone number for Follow Me communication. If using the SMS Follow Me feature, this number must be for a cellular phone with the capability to receive SMS messages.

You may only access Follow Me programming if the protocol for Account 3 is programmed as SMS or TWA Follow Me.

4.6: Event Log

The event log records the last 256 events the system has undergone. The log uses the FIFO (First In, First Out) method, automatically erasing the oldest event when the log is full.

To view the event log:

1. From the Event Log menu, select View Log [61]; a summarized version of the most recent event is displayed. Press the 💡 key to view the time/date stamp or the device/user number on the second row of the display.
2. Use the arrow keys to scroll through the events.
3. When you have finished viewing, press ×to exit the log.

The event log displays the following information for each event:

- The event descriptor – a brief description of the event that occurred.
- The zone where the event occurred.
- Time/date stamp – the exact time the event occurred.
- Report details – a single character indicating whether the event was reported to the monitoring station. The options available are **R**: Report Sent, **F**: Report Failed, **C**: Report Cancelled or **N**: No Report.

❶ Event Descriptor

❷ Time/Date Stamp

❸ Report Details

Figure 4.2: Detailed Event Log Display

Figure 4.2 shows the detailed event log entry for a Fire alarm on November 14th 2007. The event was successfully reported to the monitoring station.

4.6.1: Event Log Authorization Levels

Every event that occurs is recorded in the event log. However, certain events are intended for the installer only. Those events include various service messages that are of little interest to the regular user. The View Log function requires you to enter either the Master or Installer code. The events that are displayed depend on which code you use to enter the log – *see Appendix C: Event Table*.

4.6.2: Clearing the Event Log

The Clear Log function erases all events from the log. After performing this function, a Clear Log event is recorded in the log. The Clear Log function is accessible using the Installer code only.

To clear the event log:

1. From the Event Log menu, select Clear Log [62]; the ***OK?*** confirmation message is displayed.
2. Press ✓; the log is cleared.

For certain versions of the ProGuard800 software, the Clear Log function may be disabled.

4.7: Service Menu

The Service menu is accessible using either the Installer or Master code. This menu includes various functions that enable you to test the system effectively.

4.7.1: Set Time & Date

The time and date are used to time stamp events in the event log. Additionally the time is also displayed on the LCD display.

To set the time:

1. From the Service menu, select Set Time/Date, Set Time [7011].
2. Enter the current time.
3. Press ✓; the time is modified.

To set the date:

1. From the Service menu, select Set Time/Date, Set Date [7012].
2. Enter the current date.
3. Press ✓; the date is modified.

The format of the time and date is defined in the System Options – see 9.6.3: Time/Date Format. If you are setting the time in 12hr format, use the ☼ key to toggle between AM and PM.

© MARMITEK

4.7.2: Message Center

The *ProGuard800* Message Center is designed to allow the user to record a short message that may be played back later by another user. After a message is recorded, ***Message Waiting*** is displayed on the LCD until the message is played back.

To play back a recorded message:

- From the Service menu, select Messages, Play Message [7021].

To record a message:

1. From the Service menu, select Messages, Record Message [7022].
2. Press ✓ to start recording the message.
3. Record your message. The message may be up to twenty seconds long.
4. Press ✓ to stop recording; the message is automatically played back and ***OK?*** is displayed.
5. Press ✓ to save your recording.

To delete a message:

1. From the Service menu, select Messages, Delete Message [7023]; ***OK?*** is displayed.
2. Press ✓; the message is deleted.

The Record and Play options can also be accessed via a convenient shortcut without needing to enter a valid user code.

To access the Record Message option from Standby mode, press ▲ then ×.

To access the Play Message option from Standby mode, press ▲ then ✓.

4.7.3: Wireless Siren Test

To test the wireless siren:

- From the Service menu, select WL Siren Test [703]; the external siren is sounded briefly.

4.7.4: Siren Test

To test the control panel's built-in siren:

- From the Service menu, select Siren Test [704]; the control panel's built-in siren is sounded briefly.

4.7.5: Interface Test

The Interface test enables you to check if the speaker, LEDs and LCD are functioning correctly.

To test the system interface:

- From the Service menu, select Interface Test [705]; a short sequence of chimes are sounded from the speaker, all LEDs flash and the LCD is tested on all connected LCD keypads.

4.7.6: Walk Test

To initiate Walk Test mode:

1. From the Service menu, select Walk Test [706]; a list of registered sensors appears.
2. Trigger each sensor; when the system receives a successful transmission from a sensor, the sensor is removed from the list.
3. When all the sensors are removed from the list, ***End Walk Test*** is displayed.
4. Press × to exit Walk Test mode.

4.7.7: Transmitters

The Transmitters menu offers two utilities that serve as a valuable aid during installation.

The first utility, TX List, is a scrollable inventory of all registered transmitters and their last reported status.

To view the TX list:

1. From the Service menu, select Transmitters, TX List [7071]; the first transmitter on the list is displayed.
2. Using the arrow buttons, scroll through the transmitter list.
3. When you have finished viewing, press ×to exit the list.

The TX list displays the following information for each transmitter:

- The zone/device number or descriptor. Press the 💡 key to toggle the display.
- The signal strength of the last received transmission.
- An abbreviation indicating the last received status of the transmitter – *see Table 4.1*.

❶ Descriptor

❷ Signal Strength

❸ Status

Figure 4.3: TX List Display

This…	Means…
OK	The transmitter is functioning correctly
TA	Tamper condition
BT	Battery low
OS	The transmitter is out of synchronization
NA	The transmitter is inactive – *see section 7.4: Supervision Time*

Table 4.1: Transmitter Status Abbreviations

In most cases, an "out of synchronization" condition indicates that an unauthorized attempt at grabbing the transmission has occurred – i.e. a previous transmission has been recorded and sent by somebody trying to violate the system.

The second utility, TX Test, enables you to identify transmitters and test their signal strength.

In TX Test mode, each time a transmission is received, the activated transmitter is displayed.

© MARMITEK

If you enter this function using the Master code, a chime is sounded every time a transmission is received. If you enter this function using the Installer code, a sequence of tones are sounded indicating the transmitter's signal strength – *see Table 4.2.* This feature helps you to determine the best location to install a transmitter.

Signal Strength	Tones
0-2	1 Tone
3-5	2 Tones
6-8	3 Tones
8-9	4 Tones

Table 4.2: Signal Strength Tones

To initiate TX Test mode:

1. From the Service menu, select Transmitters, TX Test [7072].
2. Activate a transmitter; the transmitter's details are displayed.
3. When you have finished, press × to exit TX Test mode.

4.7.8: Audio Volume

To adjust the sensitivity of the microphone and the volume of the speaker:

1. Establish a two-way audio connection.
2. From the Service menu, select Audio Volume [708].
3. Adjust the setting according to the following table.

Press…	To…
1	Increase microphone sensitivity
4	Reduce microphone sensitivity
3	Increase speaker volume
6	Reduce speaker volume

Table 4.3: Voice Level Adjustment

4. Press ✓; the new settings are stored in the memory.

4.7.9: GSM Signal Strength

You can measure the GSM signal strength using the system's RSSI (Received Signal Strength Indication) meter. This function enables you to calculate the optimal location to install the control panel with the Cellular Communications module.

To view the GSM signal strength reading:

- From the Service menu, select GSM Signal [709]; the signal strength of the cellular network is displayed.

This Reading…	Means…
8 to 9	The location is good
5 to 7	The location is acceptable
Less than 5	Unacceptable – *choose another location!*

Table 4.4: GSM Signal Strength

For Remote Programming over GSM, a signal strength of 7 and above is required.

4.7.10: Display Version

To display the system's software and hardware versions.

- From the Service menu, select Version [710]; the hardware (HW) and software (SW) versions are displayed.

4.7.11: Enable Programming

The Enable Programming command enables a user with Master code authorization to grant access to system programming. This feature is relevant only if the Installer Access and/or the RP Access options are programmed as "User Initiated" – *see 9.14: Installer Access and 10.4.4: RP Access Options*.

To grant access to the installer or remote programmer:

- From the Service menu, select Enable Prog. [711]; a 30-minute time window is opened during which the Installer Code is valid or RP communication may be established.

4.7.12: Global Chime

The Chime feature causes the control panel's built-in siren to ring when specific zones are triggered. Using the Global Chime option, you can enable or disable this feature for all zones that are defined as Chime enabled – *see 7.6.4: Chime*.

To enable or disable Global Chime:

1. From the Service menu, select Global Chime [712].
2. Select either Enabled or Disabled.
3. Press ✓ when the desired setting is displayed.

Though the Service menu is accessible to the Master and Installer only, Global Chime can also be accessed via a convenient shortcut without needing to enter a valid user code. To access the Global Chime option from Standby mode, press ▲ then ▼.

© MARMITEK

Chapter Five: Telecontrol and Two-Way Audio

The *ProGuard800* control panel offers a range of Telecontrol features that provide remote access via the telephone. These features include Two-Way Audio, remote arming/disarming and cancel siren activation. This chapter explains these features and their operation procedures.

Telecontrol features can be separated into two fundamental groups; incoming and outgoing calls. These groups differ in their associated features.

5.1: Incoming Calls

The control panel can receive incoming calls from either the user or monitoring station operator. Users may use this feature as a convenient way of contacting their family, operating their system or to check their home when they are away. Additionally, the monitoring service can contact the user in the event of an emergency or use this feature for listen-in alarm verification.

For any of the incoming Telecontrol features to function, Telecontrol must be enabled in the Communication Options section of the Programming menu – *see 10.6.10: Incoming Calls*.

5.1.1: User Code Verification

To prevent unauthorized attempts to connect with the control panel, there are two user codes designed for use with the Telecontrol features. The Telecontrol code enables the user to establish communication with the control panel at any time. Additionally, the Monitoring station TWA Code is used exclusively for Two-Way Audio alarm verification and is only valid for a ten-minute period following an alarm.

5.1.2: Incoming Calls via PSTN

In the case of PSTN communication, the control panel often shares a line with regular telephone handsets, an answering machine or a fax machine. It is therefore important that the control panel distinguish between calls so that it knows when to pick up the relevant call. For this purpose the *ProGuard800* employs a double call method.

To connect to the control panel using the double call method:

1. Dial the telephone number of the line connected to the control panel.
2. Wait for two or three rings and hang-up.
3. Wait at least five seconds and dial the number again; on the second ring, the control panel picks up and sounds two DTMF tones.

5.1.3: Incoming Calls via a Cellular Network

The Cellular Communications Module has its own individual telephone number and therefore, the double call method is not needed. In this case, the user or monitoring station operator may call the control panel directly.

5.1.4: Telecontrol Call Procedure

The following procedure explains how to make a Telecontrol call. The conditions and procedure differ when using PSTN or Cellular communication. For further information, read sections 5.1.1, 5.1.2. and 5.1.3 above.

To make a Telecontrol call:

1. Call the control panel either using the double call method (PSTN) or directly (Cellular); when the control panel picks up, two DTMF tones are sounded.
2. Enter the Telecontrol code (Code 29) on your telephone within 15 seconds.

Do not enter your user code until you hear the two DTMF tones. Any digits entered before the tones are sounded are disregarded by the system.

3. A DTMF tone is sounded to indicate that the system is ready to receive commands.

   The following DTMF commands are available:

   - Press "**2**" for Two-Way Audio.
     - If the TWA mode is defined as "Simplex" (see 10.6.12: TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "**1**" on your telephone. To switch back to Listen mode, press "**0**" on your telephone.
   - Press "**3**" to fully arm the system.
   - Press "**4XX**" to turn HA unit #XX ON
   - Press "**5XX**" to turn HA unit #XX OFF
   - Press "**6**" to disarm the system.
   - Press "**9**" to cancel the siren.

The commands "3" (Full Arm),"4" (HA On), "5" (HA Off), "6" (Disarm) and "9" (Bell Cancel) can also be executed at any time during a Two-Way Audio session.

4. The duration of the call is determined by the TC/VM Timeout (see 10.6.11: Telecontrol/Vocal Message Timeout). Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "**7**" on your telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, press "*" then "**#**" on your telephone.

5.1.5: Arm/Disarm DTMF Commands

During a Telecontrol call, you can arm and disarm the system remotely using the DTMF commands "**3**" (Arm) and "**6**" (Disarm). When arming the system in this way, the system is armed immediately without an exit delay.

5.1.6. HA DTMF commands

During a Telecontrol call, you can turn On and Off the Home Automation units using the DTMF commands "**4XX**" (HA unit #XX On) and "**5XX**" (HA unit #XX Off).

© MARMITEK

5.1.7: Siren Muting

The siren is muted during Two-Way Audio communication. At the end of the call, the siren is re-activated (if the Siren Cut-Off has not yet expired). During the call, pressing "**9**" on your telephone cancels the re-activation of the siren.

5.1.8: Monitoring station Two-Way Audio

Monitoring station Two-Way Audio is an alarm verification feature that enables the monitoring station operator to establish Two-Way Audio communication with the control panel within ten minutes of an alarm.

To make a Monitoring station TWA call:

1. Call the control panel either using the double call method (PSTN) or directly (Cellular); when the control panel picks up, two DTMF tones are sounded.
2. Enter the Monitoring station TWA code (Code 30) on your telephone within 15 seconds.

Do not enter your user code until you hear the two DTMF tones. Any digits entered before the tones are sounded are disregarded by the system.

3. If the TWA mode is defined as "Simplex" (see 10.6.12: TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "**1**" on your telephone. To switch back to Listen mode, press "**0**" on your telephone.
4. The duration of the call is determined by the TC/VM Timeout (see 10.6.11: Telecontrol/Vocal Message Timeout). Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "**7**" on your telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, press "*" then "**#**" on your telephone.

5.2: Outgoing Calls

The *ProGuard800* control panel can make Two-Way Audio calls to the user or monitoring station in the event of an alarm. This feature is designed for applications such as alarm verification, panic and medical emergency.

5.2.1: Service Call

The Service Call feature enables the user to establish a two-way audio connection with the monitoring station operator. For further information on how to program this feature, see section 10.5: Service Call.

Figure 5.1: Service Call Key

To initiate a Service Call:

- Press and hold down the Service Call key for a few seconds.

If the TWA mode is defined as "Simplex" (see 10.6.12: TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). The operator may switch to Speak mode, by pressing "**1**" on their telephone. Pressing "**0**" switches back to Listen mode.

5.2.2: TWA Alarm Reporting

In the event of Burglary, Fire and Medical alarms, the control panel is able to report the events and then stay on the line after ACK 2 is received. This allows the operator to verify the alarm or provide assistance in the event of an emergency.

For this feature to function, you must enable Two-Way Audio for both the account and the event group.

The sequence for Two-Way Audio during alarm reporting is as follows:

1. An alarm event is sent to the monitoring station and acknowledgment is received (ACK 2).
2. If Two-Way Audio is enabled for the account and event group, the control panel stays on the line and opens the audio channel.
3. If the TWA mode is defined as “Simplex” (see 10.6.12: TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). The operator may switch to Speak mode, by pressing “**1**” on their telephone. Pressing “**0**” switches back to Listen mode.
4. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, the operator presses “**7**” on their telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, the operator presses “*****” then “**#**” on their telephone.

If multiple events are sent, the control panel sends all the events before opening the audio channel.

When using the SIA protocol for event reporting, this feature functions in “listen-in” mode only.

5.2.3: Two-Way Audio after Vocal Messages

If Two-Way Audio is enabled for a Vocal Message account, the user can open the audio channel by pressing “**2**” on their telephone after the system has played all of the event messages.

The sequence for Two-Way Audio after a vocal message is as follows:

1. An event occurs and the control panel calls the telephone number of VM Account 1.
2. When the user answers the call, the Home ID message and the relevant event message are played.
3. If Two-Way Audio is enabled for the VM account, the user presses “**2**” on their telephone to open the audio channel.
4. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, the user presses “**7**” on their telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, the user presses “*****” then “**#**” on their telephone.

© MARMITEK

5.2.4: TWA Follow-Me

The TWA Follow-Me feature is designed to establish a Two-Way Audio connection with the user in the event of an alarm. For this feature to function, the account's protocol must be defined as TWA Follow-Me.

The sequence for a Two-Way Audio Follow-me call is as follows:

1. An alarm occurs.
2. The control panel dials the programmed telephone number and sounds two DTMF tones when you pick up the call.
3. Press any key on your telephone; the control panel opens the audio channel.

If you press "9" to answer the call, the control panel simultaneously cancels the siren when opening the audio channel.

4. If the TWA mode is defined as "Simplex", (see 10.6.12: TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "**1**" on your telephone. To switch back to Listen mode, press "**0**" on your telephone.
5. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "**7**" on your telephone. This command restarts the timeout.
6. To disconnect before the end of the timeout, press "*****" then "**#**" on your telephone.

Chapter Six: X-10 Home Automation Control

The purpose of this chapter is to explain the various methods used to control X-10 Home Automation (HA) units installed around the home. For further information on the X-10 protocol and the choice of options that are available in programming, see *Chapter Eleven: Home Automation Programming.*

6.1: Keypad Control

Using either the front panel keypad or the wireless keypad, you can control HA units with the dedicated Home Automation keys – *see Figure 6.1*.

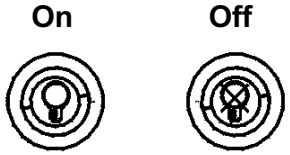


Figure 6.1: LCD Keypad Home Automation Keys

To control HA units via the front panel keypad or the wireless keypad:

1. Press one of the two Home Automation keys on the keypad (On or Off).
2. Enter the number of the required HA unit in two-digits (01-16); the command is sent to the HA unit.

To control HA units via the HK855 Hardwire LCD Keypad:

1. From the main menu, select Home Automat. [3]; HA Unit #1 is displayed.
2. Use the arrow keys to scroll to the unit you want to control.
3. Press ✓ to select the HA unit.
4. Use the arrow keys to toggle the ON/OFF command.
5. Press ✓ to select the command.
6. Scroll to the next unit you want to control or press × to exit this feature.

6.2: Keyfob Control

You can control up to two different HA units using any of the four button Keyfobs registered to the system. For further information on how to assign Keyfob buttons to HA units, see section *7.7.2: Button Assignment*.

6.3: Telephone Control

You can send On and Off commands to HA units using SMS messages sent from a cellular phone to the cellular communications module. Alternatively, the HA unit can be controlled by using DTMF commands during Telecontrol call (either to the cellular or PSTN communications modules). For this feature to function correctly, Telephone control must be enabled for the specific HA units you want to control – see *11.2.6: Telephone Control*

6.3.1: DTMF command

Using the Telecontrol feature, you can turn on and off the HA units via the telephone with DTMF commands. For further information on the Telecontrol features, see *Chapter Five: Telecontrol* and *5.1.6. HA DTMF commands*.

© MARMITEK

6.3.2: SMS Command Format

Each SMS command contains the following elements:

- ❶ SMS Command Descriptor (up to 43 characters of free text)
- ❷ # (delimiter – separates the descriptor from the actual command)
- ❸ User Code (4 digits)
- ❹ Command (0=Off, 1=On)
- ❺ Device Number (HA Units: 01-16)

The following example shows the format of an SMS command to switch on a water boiler controlled by HA unit 8.

❶									❷	❸				❹	❺	
B	**o**	**i**	**l**	**e**	**r**		**O**	**n**	**#**	**1**	**2**	**3**	**4**	**1**	**0**	**8**

While the SMS Command Descriptor is optional, you must start the SMS command with the # symbol for the system to accept the command.

6.3.3: SMS Confirmation Message Format

After an SMS command is executed, the system can return a confirmation SMS message to the sender. This message includes the HA unit's descriptor and the command that was sent. For further information on how to enable this feature, see *10.7.5: SMS Confirmation*.

The following example shows the confirmation message the sender receives for the sample command from the previous section.

B	**O**	**I**	**L**	**E**	**R**	**-**	**O**	**N**

6.4: Scheduling

Scheduling allows you to program the panel to send On/Off commands to HA units at specific times. You can also program the days of the week that the schedule is active.

6.4.1: On Time

To edit an HA unit's "On" Time:

1. From the main menu, select HA Schedules [8].
2. Select an HA unit.
3. From the X-10 unit's sub-menu, select On Time [#1].
4. Enter a time (HH:MM).
5. Press ✓ when the desired setting is displayed.

6.4.2: Off Time

To edit an HA unit's "Off" Time:

1. From the main menu, select HA Schedules [8].
2. Select an HA unit.
3. From the HA unit's sub-menu, select Off Time [#2].
4. Enter a time (HH:MM).
5. Press ✓ when the desired setting is displayed.

6.4.3: Weekly Schedule

To program the days of the week that the schedule is active:

1. From the main menu, select HA Schedules [8].
2. Select an HA unit.
3. From the HA unit's sub-menu, select Schedule [#3].
4. Use keys 1 to 7 to toggle the days on and off.

Press…	To toggle…
1	Sunday
2	Monday
3	Tuesday
4	Wednesday
5	Thursday
6	Friday
7	Saturday

Table 6.1: Weekly Schedule

5. Press ✓ when the desired setting is displayed.

© MARMITEK

Chapter Seven: Devices

This chapter explains how to register devices to the system and the programming options for each device. For further information, please refer to the installation instructions included with each device.

7.1: Device Registration

For the system to recognize individual devices, each device must be registered to the system. For example, if the device is a wireless transmitter, registration enables the system to identify the source of a received transmission. Each device has an individual encrypted ID code. Registering the device to the system familiarizes the system with this code.

It is not necessary to register hardwire sensors connected to Zone 33.

To register a device to the system:

1. From the Programming menu, select Devices [91].
2. Select the type of transmitter you want to register. For example, if you want to register a wireless sensor to a zone, select Zones.
3. Select the specific device you want to register (for example, Zone 4); the system initiates Registration mode. During Registration mode, the system waits for two transmissions from the device.

If a device has already been registered at the required location, the system will not initiate Registration mode. If the device has already been registered at another location, attempts to register are ignored by the system

4. Register the device – *refer to each device's installation instructions in Appendix B for further details.*
5. When two transmissions have been received, ***Save?*** is displayed.
6. Press ✓to confirm registration, or × to cancel.

7.2: Device Descriptors

You can assign a 16-character descriptor to each device except the wireless siren. These descriptors help identify the devices when you operate and program the system.

To edit a device descriptor:

1. From the Programming menu, select Devices [91].
2. Select a device type.
3. From the device's sub-menu, select Descriptor.
4. Edit the descriptor using the alphanumeric keypad.
5. Press ✓ when you have finished editing.

7.3: Device Deletion

When you want to remove a device from the system, you have to delete the device. It is important to delete unused devices for two reasons. Firstly, you have to delete a device before you can register a new transmitter in its place. Secondly, if the device is a wireless sensor, it is important to delete the device so that the system will not react to the transmitter's failure to send supervision signals.

To delete a device:

1. From the Programming menu, select Devices, [91].
2. Select the type of wireless device you want to delete.
3. From the device's sub-menu, select Delete.
4. Press ✓ to confirm; the device is deleted.

7.4: Supervision Time

The sensors in Marmitek's ProGuard800 supervised wireless range send a supervision signal approximately one hour after its last transmission. If the system does not receive supervision signals from a specific transmitter, the transmitter is regarded as inactive.

The amount of time after which a transmitter is considered inactive is called the Supervision Time. There is a separate supervision time for general transmitters and devices that are registered to Fire zones.

To program the Supervision Time for general transmitters:

1. From the Programming menu, select Devices, Superv. Time, General [9161].
2. Enter a supervision time between 04:00 and 23:59 hours.

To program the Supervision Time for transmitters registered to Fire zones:

1. From the Programming menu, select Devices, Superv. Time, Fire [9162].
2. Enter a supervision time between 02:00 and 23:59 hours.

7.5: Re-Synchronization

Transmissions that are out of synchronization are rejected by the system. For example, it is not possible to arm or disarm the system using a keyfob that is out of synchronization. In the event that a transmitter is out of synchronization, it is possible to re-synchronize the transmitter and restore normal operation.

To re-synchronize transmitters:

1. From the Programming menu, select Devices, TX Re-synch [917]; a 10-minute time window is opened.
2. During the 10-minute time window, if a transmission is received that is out of synchronization, the transmitter is re-synchronized.

7.6: Zones

The *ProGuard800* includes 33 security zones. Zones 1-32 are intended for wireless sensors. One sensor can be registered to each wireless zone. The system supports Marmitek's ProGuard800supervised wireless range of transmitters that includes various PIR sensors, magnetic contacts and smoke detectors. All these transmitters send supervision signals to the panel's receiver in order to indicate that the transmitter is functional.

Zone 33 is an on-board hardwire zone. This zone is programmed in the same way as the wireless zones with the exception of registration and deletion.

© MARMITEK

This section explains the sections of programming exclusive to sensors. For information on registration, descriptor editing and deletion, see sections 7.1, 7.2 and 7.3, respectively.

7.6.1: Zone Type

The zone type defines the type of alarm the system generates when the sensor is tripped.

To program a zone type:

1. From the Programming menu, select Devices, Zones [911].
2. Select the sensor you want to program.
3. From the sensor's sub-menu, select Zone Type [#02].
4. Select one of the following zone types:

   - Normal
   - Entry/Exit
   - Follower
   - Panic
   - Medical
   - Fire
   - 24Hr
   - 24Hr-X (future option)
   - Gas
   - Flood
   - Environmental
   - No Motion
   - Not Used

   For a detailed explanation on the function of each zone type, see Appendix D: Zone Types

7.6.2: Arm Set

The Arm Set option allows you to define the arming methods in which the zone is included.

To program the Arm Set option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the sensor you want to program.
3. From the zone's sub-menu, select Arm Set [#03]; the zone's current Arm Set setting is displayed.

Arm Set	Description
1 (F)	The zone is included in Full arming.
2 (P)	The zone is included in Part arming.
3 (PE)	The zone is included in Perimeter arming.

Table 7.1 Arm Set Options

4. Use the keys 1, 2 and 3 to toggle the current setting.
5. Press ✓ when the desired setting is displayed.

It is not necessary to program this option for Panic, Medical, Fire, 24Hr, Gas, Flood and Environmental zones.

7.6.3: Bell

Each zone can be programmed to activate the siren when triggered or to generate a silent alarm where only a message is sent to the monitoring station.

To program the Bell option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Bell [#05]; the zone's current Bell setting is displayed.

4. Select either Enabled or Disabled.

Fire zones always activate the siren regardless of what is programmed for this option.
If the bell is disabled for Panic zones, this also disables all forms of alarm indication from the on-board keypad in the event of a Panic alarm.
If the Bell option is enabled for Environmental or Flood zones, the system sounds trouble tones from the keypad.

7.6.4: Chime

When Chime is enabled, triggering the zone when the system is disarmed causes the internal siren to chime.

To program the Chime option:

1. From the Programming menu, select Devices, Sensors [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Chime [#06]; the zone's current Chime setting is displayed.
4. Select either Enabled or Disabled.

7.6.5: Force Arm

Force arming enables you to arm the system when the system is not ready. For example, a door that is protected by a magnetic contact is open. You may arm the system on condition that the zone is defined as Force Arm enabled. This door must be closed by the end of the Exit delay otherwise an alarm is generated. If the magnetic contact's zone is defined as Force Arm disabled, the system will not be ready to arm until you close the door.

To program the Force Arm option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Force Arm [#07]; the zone's current Force Arm setting is displayed.
4. Select either Enabled or Disabled.

For the Force Arm feature to function, you must also enable Force Arming in System Options (see 9.3.1: Forced Arm).

7.6.6: Swinger

A zone defined as Swinger enabled can generate only a limited number of alarms during a specific time period. The Swinger setting is defined in System Options – *see 9.1: Swinger Setting.*

To program the Swinger option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Swinger [#08]; the zone's current Swinger setting is displayed.
4. Select either Enabled or Disabled.

Do not enable the Swinger option for zones that are always active (Panic, Medical, Fire, 24-hr, Gas, Flood and Environmental zones).

© MARMITEK

7.6.7: Repeater

The RP835 repeater is an additional module that extends the range of the wireless transmitters. For a sensor to use the repeater to relay transmissions to the system, you must define the Repeater option for its zone as “Use Repeater”.

To program the Repeater option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone’s sub-menu, select Repeater [#09]; the zone’s current Repeater setting is displayed.
4. Select either No Repeater or Use Repeater.

7.7: Keyfobs

The *ProGuard800* supports two types of Keyfob transmitter, PR811 and KR814. You can register up to 19 Keyfobs to the system. Figure 7.1 illustrates these transmitters and the functions assigned to their buttons. For information on registration, descriptor editing and deletion, see sections 7.1, 7.2 and 7.3, respectively.

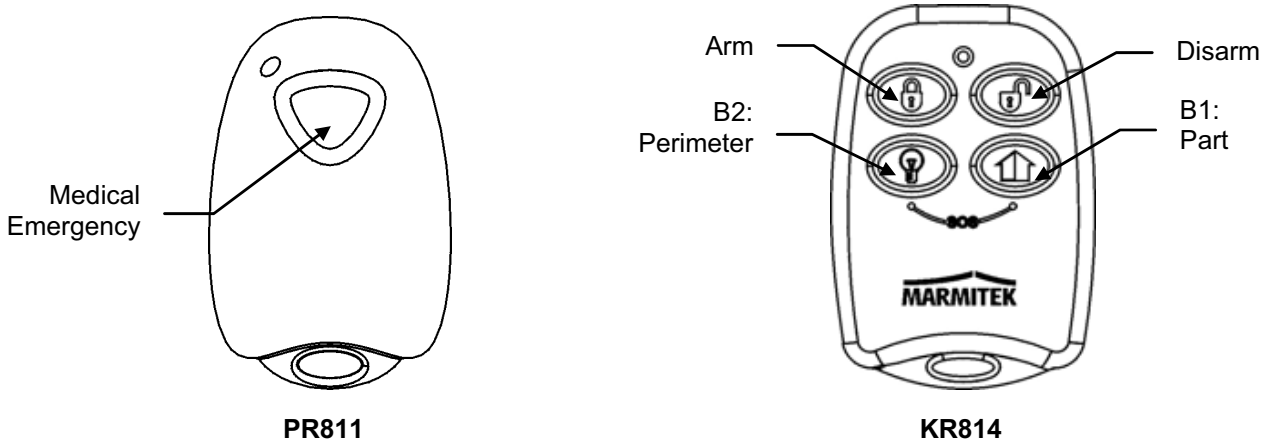


Figure 7.1: Keyfob Button Assignments

The following sections explain the programming options exclusive to the KR814 Keyfob transmitter. These programming options are not relevant to the PR811.

7.7.1: Keyfob Type

You can define each registered Keyfob as Controlled or Non-controlled. A Controlled Keyfob causes the system to send arm/disarm event messages to the monitoring station. Non-controlled Keyfobs never send arm messages and send a disarm message only if the system is disarmed after an alarm occurrence.

To program a Keyfob type:

1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the Keyfob you want to program.
3. From the keyfob’s sub-menu, select Type [#2]; the current setting is displayed.
4. Select either Controlled or Non-controlled.

7.7.2: Button Assignment

The KR814 includes two buttons (B1 and B2) that you can program individually. The default functions for B1 and B2 offer different arming methods. Alternatively, you can program these buttons to control a specific HA unit.

To program buttons B1 and B2:

1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the Keyfob you want to program.
3. From the keyfob's sub-menu, select either B1 Assign [#4] or B2 Assign [#5].
4. Select the HA unit you want the button to control (01-16) or enter 00 to program the button's default function.

   The default functions are as follows:
   B1: Part arming
   B2: Perimeter arming

7.7.3: SOS Panic Alarm Activation (KR814)

Using the four-button Keyfob, you can activate an SOS Panic alarm by pressing two buttons simultaneously. Figure 7.2 illustrates how to activate an SOS Panic alarm on the KR814 wireless Keyfob.

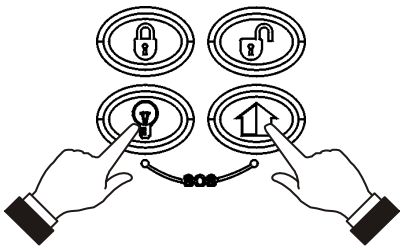


Figure 7.2: SOS Panic Alarm Activation

7.8: Keypads

Up to four wireless keypads are supported by the system. With the exception of the Cancel key, operation is identical for both WK820 and RC840 keypads. For information on registration, descriptor editing and deletion, see sections 7.1, 7.2 and 7.3, respectively.

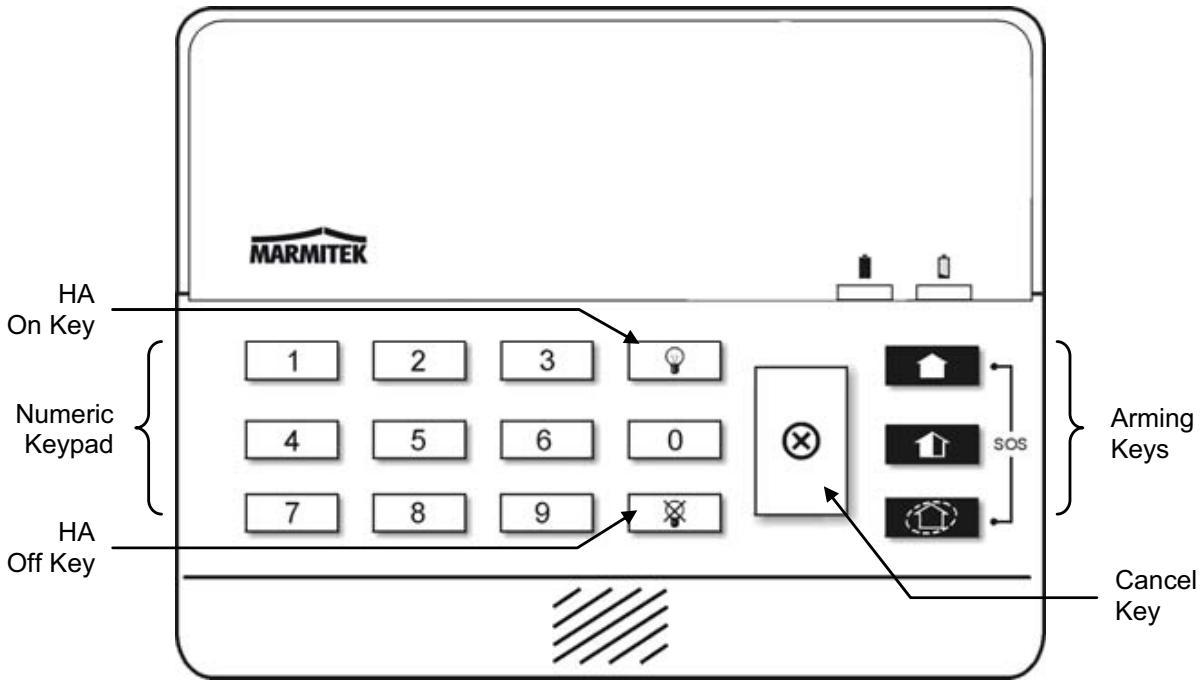
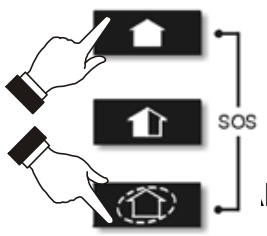


Figure 7.3: WK820 Keypad Layout



7.8.1: Keypad SOS Panic Alarm Activation

Using any of the wireless keypads, you can activate an SOS Panic alarm by pressing the Full and Perimeter arming keys simultaneously. Figure 7.4 illustrates how to activate an SOS Panic alarm on the WK820 wireless keypad.

7.9: Repeaters

Repeaters are designed to extend the wireless range of the control panel. Up to four repeaters may be registered to the system with a maximum of 32 transmitters associated with each receiver. For information on registration, descriptor editing and deletion, see sections 7.1, 7.2 and 7.3, respectively.

7.10: Wireless Siren

For the wireless siren to function, the control panel must have the on-board transmitter installed on the Main board – *see 1.4.1: The Main Board* for the location of the on-board transmitter connector.

Using this transmitter, the system sends alarm and arm status information to the wireless siren's receiver. This requires that you register the transmitter to the wireless siren's receiver.

To register the on-board transmitter to the wireless siren's receiver:

1. Set the wireless siren's receiver to Registration mode – *refer to the siren's installation instructions for further information*.
2. Activate the siren using the WL Siren Test feature – *see 4.7.3: Wireless Siren Test.*
3. Activate the siren again; the on-board transmitter is registered to the siren's receiver.

When installing 2-way sirens, the wireless siren also includes a transmitter that must be registered to the control panel. For information on registration and deletion, see sections 7.1 and 7.3, respectively.

7.10.1: Wireless Siren Type

The control panel supports both 1-way and 2-way wireless sirens. For this feature to function correctly, you must define the wireless siren type in programming.

The following options are available:

- 1-Way Siren – if using the ProGuard800 SI825 status indicator.
- 2-Way Siren – if using the OS826 wireless siren.
- 2-Way Siren/Kpd – if using the OS826 wireless siren and the 2-way WK820SI keypad (this option is for future use).

To program the wireless siren type:

1. From the Programming menu, select Devices, Siren, WL Siren Type [9152].
2. Select a siren type or No WL Siren if no siren is installed.

7.10.2: Wireless Siren Delay

The Wireless Siren Delay is the period of time during which the wireless siren is not sounded after an alarm is triggered by normal, follower or 24Hr zones. This feature is implemented only when the system is not fully armed. During the Wireless Siren Delay, the control panel's built-in siren is sounded but the alarm report is not sent until the delay has expired. This gives the user enough time to disarm in the event that the alarm was accidentally triggered during Part or Perimeter arming. If the user disarms the system during the Siren Delay, an alarm event is not reported to the monitoring station.

To program the Wireless Siren Delay time:

1. From the Programming menu, select Devices, Siren, WL Siren Delay [9153].
2. Enter a Siren Delay time (00-63 seconds).
3. Press ✓ when the desired setting is displayed.

7.10.3: Siren Cut-Off

The Siren Cut-Off is the period of time the sirens are activated after an alarm has occurred. You may program a Siren Cut-Off time of between ten seconds to twenty minutes.

To program the Siren Cut-Off time:

1. From the Programming menu, select Devices, Siren, Cut-Off [9154].
2. Enter a Siren Cut-Off time (00:10 - 20:00).
3. Press ✓ when the desired setting is displayed.

7.10.4: Wired Siren

When the system generates an audible alarm, both the wired built-in siren and the wireless siren are sounded. This option allows you to disable the alarm from the control panel's built-in siren. If disabled, the control panel's built-in siren may still be used to sound arm/disarm and entry/exit tones.

To program the Wired Siren option:

1. From the Programming menu, select Devices, Wired Siren [9155].
2. Select Enabled or Disabled.

7.11: Smartkeys (for future use)

Smartkeys enable the user to arm and disarm the system without needing to enter a code. You can register up to 16 smartkeys to the system. For information on registration, descriptor editing and deletion, see sections 7.1, 7.2 and 7.3, respectively.

7.11.1: Smartkey Type

You can define each registered smartkey as Controlled or Non-controlled. A Controlled smartkey causes the system to send arm/disarm event messages to the monitoring station. Non-controlled smartkeys never send arm messages and send a disarm message only if the system is disarmed after an alarm occurrence.

To program the smartkey type:

1. From the Programming menu, select Devices, Smartkeys [918].
2. Select the smartkey you want to program.
3. From the smartkey's sub-menu, select Type [#2]; the current setting is displayed.
4. Select either Controlled or Non-controlled.

© MARMITEK

Chapter Eight: Entry/Exit Timers and System Tones

This chapter explains how to program the time of the Entry/Exit delays and the tones sounded by the built-in siren and wireless siren during Exit/Entry delays, arming, disarming, home automation operation and when a trouble condition is present.

8.1: Entry/Exit Delay

The Entry/Exit delay timers determine the amount of time the user has to arm or disarm the system before an alarm is activated.

You can program separate Entry and Exit delays for each arming method.

To program Exit delay timers:

1. From the Programming menu, select Entry/Exit, Exit Delays [921].
2. Select the Exit delay you want to program: Full [#1], Part [#2] or Perimeter [#3].
3. Enter a delay time (000-255 seconds).
4. Press ✓ when the desired setting is displayed.

To program Entry delay timers:

1. From the Programming menu, select Entry/Exit, Entry Delays [922].
2. Select the Entry delay you want to program: Full [#1], Part [#2] or Perimeter [#3].
3. Enter a delay time (000-255 seconds).
4. Press ✓ when the desired setting is displayed.

8.2: Arm on Exit

The Arm on Exit feature cancels the unnecessary remainder of the Exit delay that continues to count down after the user has vacated the premises. This feature automatically arms the system when an Entry/Exit zone is closed during the Exit delay.

To program the Arm on Exit option:

1. From the Programming menu, select Entry/Exit, Arm On Exit [923].
2. Select Enabled or Disabled.

8.3: Supplementary Entry Delay

The Supplementary Entry Delay is a pre-alarm feature that is employed in the event that the system is not disarmed during the entry delay. When the entry delay expires, the control panel's built-in siren is sounded during an additional entry delay period. At the end of the supplementary entry delay, the system generates a full alarm condition; the wireless siren is sounded and an alarm event is reported to the monitoring station.

To program the Supplementary Entry Delay setting:

1. From the Programming menu, select Entry/Exit, Supp. Ent. Delay [924].
2. Select Enabled or Disabled.

8.4: Entry Deviation

Entry Deviation is a pre-alarm feature employed in the event that a sensor defined with the “Normal” zone type is opened during the entry delay. In this case, the control panel’s built-in siren is sounded until the end of the entry delay period. Failure to disarm by the end of the entry delay causes the system to generate an alarm.

To program the Entry Deviation setting:

1. From the Programming menu, select Entry/Exit, Ent. Deviation [925].
2. Select Enabled or Disabled.

8.5: Exit Restart

Exit Restart is a feature that is designed to prevent false alarms caused by user error during exit. If this feature is enabled, re-opening a closed Entry/Exit zone during the remainder of the Exit delay causes the Exit delay to re-start. For example, the Exit delay is programmed as 60 seconds. The user arms the system and leaves the premises. With 10 seconds remaining, the user re-enters the premises and the Exit delay starts to count down again from 60 seconds.

To program the Entry Deviation setting:

1. From the Programming menu, select Entry/Exit, Exit Restart [926].
2. Select Enabled or Disabled.
3. Press ✓ when the desired setting is displayed.

8.6: Arming Tones

Arming tones are the tones sounded by the control panel’s built-in siren and/or the wireless siren when arming and disarming the system. Each set of tones can be enabled or disabled according to the requirements of the installation.

8.6.1: Exit Delay Tones

To program tones sounded by the wireless siren during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, WL Siren [9311].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, Siren [9312].
2. Select No Tones, Four Tones or Continuous Tones.

8.6.2: Entry Delay Tones

To program tones sounded by the wireless siren during the Entry delay:

1. From the Programming menu, select Tones, Entry Tones, WL Siren [9321].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren the Entry delay:

1. From the Programming menu, select Tones, Entry Tones, Siren [9322].
2. Select No Tones, Four Tones or Continuous Tones.

8.6.3: Arming Tones

To program tones sounded by the wireless siren on arming:

1. From the Programming menu, select Tones, Arm Tones, WL Siren [9331].

© MARMITEK

2. Select Enabled or Disabled.

To program tones sounded by the built-in siren on arming:

1. From the Programming menu, select Tones, Arm Tones, Siren [9332].
2. Select Enabled or Disabled.

8.6.4: Disarming Tones

To program tones sounded by the wireless siren on disarming:

1. From the Programming menu, select Tones, Disarm Tones, WL Siren [9341].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren on disarming:

1. From the Programming menu, select Tones, Disarm Tones, Siren [9342].
2. Select Enabled or Disabled.

8.7: Home Automation Tones

Home Automation tones are sounded when you control HA units using keypads or keyfob transmitters.

To program built-in siren Home Automation tones:

1. From the Programming menu, select Tones, HA Tones [935].
2. Select Enabled or Disabled.

8.8: System Trouble Tones

System trouble tones are sounded to provide an audible indication that a system trouble condition exists. On hearing these tones the user is then able to determine which trouble condition is present from the LCD keypad on the front panel. For additional information, see 3.4.2: System Trouble Tones.

8.8.1: Trouble Tones

The Trouble Tones option allows you to enable or disable audible trouble annunciation.

To program the Trouble Tones option:

1. From the Programming menu, select Tones, Trouble Tones [936].
2. Select Enabled or Disabled.

8.8.2: Telephone Trouble Tones

Most trouble tones are not sounded between 10:00pm and 7:00am so as not to disturb the user late at night. Telephone trouble, however, may be an attempt to sabotage the system by cutting the telephone wires. For this reason, you can program telephone trouble tones to sound at all times.

To program the Telephone Trouble Tones option:

1. From the Programming menu, select Tones, Tel. Trb. Tones [937].
2. Select Immediate or Delayed.

8.8.3: Fire Trouble Tones

The Fire Trouble Tones option is a feature designed to repeat fire-related trouble tones until the problem has been taken care of. If this feature is enabled, fire trouble tones shall be repeated 3½ hours after the user has manually silenced the tones if the trouble condition has not been restored.

To program the Fire Trouble Tones option:

1. From the Programming menu, select Tones, Fire Trb. Tones [938].
2. Select Enabled or Disabled.

It is not necessary to program the Telephone Trouble Tones and Fire Trouble Tones options if the Trouble Tones option is programmed as disabled.

8.9: Tones Options

8.9.1: Tones Output

The Tones Output option enables you to determine whether the tones sounded when arming and disarming are sounded by the control panel's built-in siren or its built-in speaker.

To program the Tones Output option:

1. From the Programming menu, select Tones, Tones Options, Tones Output [9391].
2. Select Siren or Speaker.

8.9.2: Speaker Volume

The Speaker Volume option determines the volume level of the tones sounded by the speaker.

To program the Speaker Volume option:

1. From the Programming menu, select Tones, Tones Options, Speaker Vol. [9392].
2. Select High or Low.

It is not necessary to program the Speaker Volume option if "Siren" is selected for the Tones Output option.

8.9.3: Keypad Selection

The Keypad Selection feature enables you to enable or disable tones sounded by hardwire LCD keypads.

To program the Keypad Selection option:

1. From the Programming menu, select Tones, Tones Options, Keypad Sel. [9393].
2. Use the 2, 3 and 4 keys to toggle keypad tones on or off for each keypad. If the number of the keypad appears on the display, tones will be sounded from that keypad.
3. Press ✓ when the desired setting is displayed.

It is not possible to disable tones for the front panel keypad (Keypad #1).

© MARMITEK

As the name suggests, System Options are settings that affect the entire system. This chapter offers explanations and programming instructions for each of these options.

9.1: Swinger Setting

A sensor defined as Swinger enabled can generate only a limited number of alarms during a specific time period or during an arming period. The following options are available:

- One alarm per arming period
- One alarm per hour
- One alarm per day
- One alarm per week
- No swinger

To program the Swinger setting:

1. From the Programming menu, select System Options, Swinger [9401].
2. Select a Swinger setting from the above list.

9.2: Code Lockout

The Code Lockout option locks the keypad for 30 minutes if five unsuccessful attempts are made to enter the user code.

To program the Code Lockout setting:

1. From the Programming menu, select System Options, Code Lockout [9402].
2. Select Enabled or Disabled.

During the 30-minute lockout period, you can still arm and disarm the system using keyfobs and smartkeys. If one key arming is enabled, you may still arm the system using the wireless keypad.

9.3: Arm/Disarm Options

The options offered in this section relate to arming and disarming the system.

9.3.1: Forced Arm

Forced arming enables you to arm the system when the system is not ready. This option allows you to enable or disable Forced arming for the entire system. Additionally, you can enable or disable Forced arming for each individual zone. For further information, see section 7.6.5: Force Arm.

To program the Forced Arm setting:

1. From the Programming menu, select System Options, Arm/Disarm, Forced Arm [94031].
2. Select Enabled or Disabled.

9.3.2: One-Key Arming

You can arm the system by pressing any of the three arming keys on the keypad. If One-Key Arming is enabled, the system does not prompt you for a user code.

To program the One-Key Arming setting:

1. From the Programming menu, select System Options, Arm/Disarm, One-Key Arming [94032].
2. Select Enabled or Disabled.

9.3.3: Supervised Arm

The Supervised Arm option is a feature designed to supervise intrusion sensor activity before you arm the system.

If the system has not received a transmission from a sensor during the interval defined for this option, all arming methods that include that sensor shall not be available.

Medical, Panic, Fire, Gas, Flood and Environmental zones are not included in this supervision and do not affect the system's ability to arm.

Press ▼ to check which sensor is causing the "System Not Ready" condition.

To make the required arming method available, activate the sensor. It is important to remember that the PIR sensors have a four-minute delay between transmissions.

If activating the sensor does not help, there may be a problem with the sensor. You can bypass the faulty sensor's zone to allow system arming until the problem is remedied.

Zone bypassing is valid for one arming period only. All bypassed zones are automatically unbypassed when the system is disarmed.

To program the Supervised Arm interval:

1. From the Programming menu, select System Options, Arm/Disarm, Superv. Arm [94033].
2. Enter a Supervised Arm interval (001-255 minutes or 000 to disable the Supervised Arm option).
3. Press ✓ when the desired setting is displayed.

Do not program a Supervised Arm interval that is less than the sensor's supervision time.

9.3.4: Instant Arming

Instant arming is a feature that allows you to cancel the entry delay after arming the system – *see 3.7.7: Instant Arming*. The feature is designed for use in situations where the system's perimeter is armed and nobody is expected to enter the premises from outside.

To enable/disable the Instant Arm option:

1. From the Programming menu, select System Options, Arm/Disarm, Instant Arming [94034].
2. Select Enabled or Disabled.

9.3.5: Keyfob Disarm

The Keyfob Disarm option enables you to determine whether it is possible for the user to disarm the system using their keyfob at all times or during the entry delay only.

1. From the Programming menu, select System Options, Arm/Disarm, KF Disarm [94035].
2. Select Always or On Entry.

© MARMITEK

9.3.6: Keyfob Arm

The Keyfob Arm option offers two options concerning the behaviour of the system when arming with a Keyfob. These options are as follows:

- With Exit Delay – when arming with a Keyfob, the system initiates the Exit delay of the chosen arming method.
- No Exit Delay – when arming with a Keyfob, the system arms instantly without initiating the Exit delay.

To program the Keyfob Arm option:

1. From the Programming menu, select System Options, Arm/Disarm, KF Arm [94036].
2. Select With Exit Delay or No Exit Delay.
3. Press ✓ when the desired setting is displayed.

9.4: Panic Alarm

SOS Panic alarms generated from the front panel, keypads or keyfobs can be defined as either audible or silent.

To program the Panic Alarm setting:

1. From the Programming menu, select System Options, Panic Alarm [9404].
2. Select Audible or Silent.

9.5: AC Loss Delay

The AC Loss Delay is the amount of time that has to elapse before an AC Loss report is sent to the monitoring station. If AC power is restored before the event message is sent, the event message is cancelled and will not be sent. You can program an AC Loss Delay to be between 1 and 255 minutes after the system first senses the AC loss condition. Alternatively you can program a random AC Loss Delay.

The AC Restore message is also sent using the same method described above. AC Restore is reported only if the AC Loss report was sent.

To program the AC Loss Delay:

1. From the Programming menu, select System Options, AC Loss Delay [9405].
2. Enter a delay time (001-255 minutes) or enter 000 if you require the system to choose a random AC Loss Delay.
3. Press ✓ when the desired setting is displayed.

9.5.1: Random AC Loss Delay

In the event of AC loss, an event message is sent to the monitoring station between 15 and 30 minutes after the AC loss condition is sensed. The system chooses this delay at random in order to prevent the monitoring station being inundated by simultaneous AC Loss reports in the event of a regional power cut.

9.6: Display Options

The following options relate to the information the system displays on the LCD keypad.

9.6.1: Arm Status Display

The Arm Status Display includes the current arm status and any trouble conditions that may exist within the system. You can program the system to display this information at all times or only for two minutes after arming or disarming the system.

To program the Arm Status Display options:

1. From the Programming menu, select System Options, Display, Arm Status [94061].
2. Select Display Always or Display 2 Min.

9.6.2: Banner

The Banner is the 16-character text that you can program to appear on the top row of the LCD display. This text replaces the arm status if it is programmed to display for two minutes only – *see 9.6.1: Arm Status Display.*

To edit the Banner text:

1. From the Programming menu, select System Options, Display, Banner [94062].
2. Edit the Banner text using the alphanumeric keypad.
3. Press ✓ when you have finished editing.

The system never displays the Banner text if the Arm Status Display option is programmed as Always.

9.6.3: Time/Date Format

This option determines the format in which the time and date are displayed.

The following options are available:

- DD/MM/YY, 24Hr
- DD/MM/YY, 12Hr
- MM/DD/YY, 24Hr
- MM/DD/YY, 12Hr

To program the Time/Date format:

1. From the Programming menu, select System Options, Display, Time Format [94063].
2. Select the required format from the options available.

9.6.4: Supervision Loss Indication

This option enables you to select whether transmitter supervision loss shall be indicated to the user in the system trouble display.

To program the Supervision Loss Indication setting:

1. From the Programming menu, select System Options, Display, SV Loss Ind. [94064].
2. Select Enabled or Disabled.

© MARMITEK

9.7: PGM Output Options

The PGM is a programmable output that is triggered according to specific system status conditions.

9.7.1: Output Trigger

The Output Trigger option determines the conditions that activate and deactivate the PGM output.

To program the Output Trigger:

1. From the Programming menu, select System Options, PGM Options, Output Trigger [94071].
2. Select an Output Trigger option from the following table.

Trigger Option	Activated by…	Deactivated by…
PGM Not Used	The PGM output is disabled	
Full Arm	System "Full" armed	System disarmed or PGM Cut-off
Perimeter Arm	System "Perimeter" armed	
Part Arm	System "Part" armed	
Arm Status	Any arming method	
Power Trouble	AC Loss or Low Battery conditions	AC restore or Battery restore
Tel. Line Trouble	Telephone line supervision trouble	Telephone line restore
System Trouble	System trouble condition	System trouble restore
Medical	Medical alarm	Any arming method, system disarmed or PGM Cut-off
Burglary	Burglary alarm	
Fire Alarm	Fire alarm	
Zone Status*	Open zones (steady) Bypassed zones (pulsing)	All zones closed and no zones bypassed
Entry/Exit	Entry/Exit delay follower	
Siren	Built-in siren follower	
WL Siren	Wireless siren follower	
Tone Follower	Keypad Tone Follower	

Table 9.1: PGM Output Trigger Options

* Functions only when the system is disarmed.

For certain trigger options, deactivation may be determined by the PGM Cut-off (see 9.12.4: PGM Cut-off). If the PGM Cut-off is programmed as 000 (continuous activation), the PGM output shall remain activated until it is toggled by the relevant change in system status.

9.7.2: Output Type

The Output Type option determines whether the PGM output produces a steady or pulsed output.

To program the Output Type:

1. From the Programming menu, select System Options, PGM Options, Output Type [94072].
2. Select Steady or Pulsed.

The Zone Status, Siren and WL Siren trigger options have a fixed Output Type; there is no need to program an Output Type for these options.

9.7.3: Polarity

You can determine the polarity of the PGM output from the following two options:

- Active High: The output is normally off and is switched on when activated.
- Active Low: The output is normally on and is switched off when activated.

To program the Output Type:

1. From the Programming menu, select System Options, PGM Options, Polarity [94073].
2. Select Active High or Active Low.

9.7.4: PGM Cut-off

The PGM Cut-off is the duration for which the PGM is activated. Certain Output Trigger types, are deactivated after the PGM Cut-off time has expired– *see Table 9.1: PGM Output Trigger Options*. For those Output Trigger types that are not affected by the PGM Cut-off, there is no need to program this option.

To program the PGM Cut-off time:

1. From the Programming menu, select System Options, PGM Options, PGM Cut-off [94074].
2. Enter a PGM Cut-off time (001-255 seconds or 000 for continuous activation).
3. Press ✓ when the desired setting is displayed.

9.8: Guard Code (for future use)

The Guard Code is a future option that is not available in the current firmware. The default setting for this option is disabled. Marmitek recommend that you do not change this setting.

9.9: "No Arm" Indication

The "No Arm" indication is a feature designed to inform the monitoring station that the system has not been armed for a specified period of time.

To define the "No Arm" indication interval.

1. From the Programming menu, select System Options, No Arm Ind. [9409].
2. Select 1 Week, 2 Weeks, 3 Weeks, 4 Weeks or Disabled.

The No Arm event message is an unclassified event. This means that it does not belong to any event group. If the No Arm option is programmed with any option other than "Disabled", the event message shall be sent.

9.10: Jamming Detection

The system is able detect RF Jamming that is usually caused by an intruder attempting to compromise the security system.

To program the Jamming Detection setting:

1. From the Programming menu, select System Options, Jamming Det. [9410].
2. Select Enabled or Disabled.

© MARMITEK

9.11: "No Motion" Time

The No Motion feature is designed to monitor the activity of disabled or elderly people. If a sensor defined as "No Motion" (see 7.6.1: Zone Type) has not detected within a pre-defined period of time, a No Motion event message is sent to the monitoring station.

To program the No Motion time:

1. From the Programming menu, select System Options, No Motion [9411].
2. Select 6 Hours, 12 Hours, 24 Hours, 48 Hours, 72 Hours or Disabled.

9.12: Microphone/Speaker Options

In addition to the built-in microphone and speaker, the *ProGuard800* control panel supports an external microphone/speaker unit called the "ProGuard800 IP850-Interphone". The Microphone/Speaker option allows you to choose which microphone and speaker are in use. You can choose one mic./speaker (internal or external) to function exclusively or both may function simultaneously.

To program the Microphone/Speaker option:

1. From the Programming menu, select System Options, Mic./Speaker [9412].
2. Select Internal, External or Internal & External.

9.13: Vocal Messages

The Vocal Messages option allows you to enable/disable vocal annunciation of system status. When this feature is enabled, the system plays a short message to announce events such as arming and disarming.

To program the Vocal Messages option:

1. From the Programming menu, select System Options, Vocal Message [9413].
2. Select Enabled or Disabled.

The availability of the Vocal Message annunciation feature is hardware dependent.

9.14: Installer Access

The Installer Access option determines if the Installer code can access the system at all times or only after the Master code provides authorization with the Enable Programming command – *see 4.7.11: Enable Programming.*

To program the Installer Access option:

1. From the Programming menu, select System Options, Instal. Access [9414].
2. Select Always or User Initiated.

9.15: Auto Log View (for future use)

Auto Log View is a future option that is not available in the current firmware. The default setting for this option is disabled. Marmitek recommend that you do not change this setting.

9.16: Daylight Savings

Using the Daylight Savings option, the system is able to automatically adjust its clock twice a year according to the national adjustment to Daylight Saving Time.

Two options are available:

- Europe – the clock is adjusted forward 1hr on the last Sunday in March at 2am, the clock is adjusted back 1hr on the last Sunday in October at 3am.
- USA– the clock is adjusted forward 1hr on the first Sunday in April at 2am, the clock is adjusted back 1hr on the last Sunday in October at 2am.

From 2007, Daylight Saving Time in the USA begins on the second Sunday in March and ends on the first Sunday of November. This modification has been accounted for in the firmware and the time shall be updated automatically according to the new dates from 2007 onwards.

To program the Daylight Savings option:

1. From the Programming menu, select System Options, Daylight Savings [9416].
2. Select Europe, USA or Disabled.

9.17: Report Fail Trouble

If the Report Fail Trouble option is enabled, failure to report an event displays System Trouble on the LCD display. Report Fail Trouble is displayed after the control panel has exhausted all message attempts and report cycles when trying to report the event. To restore a System Trouble condition caused by failure to report, press ▼ until you have scrolled through the entire system trouble list. If the Report Fail Trouble is disabled, failure to report an event does not cause a system trouble condition.
To program the Report Fail Trouble option:

1. From the Programming menu, select System Options, Rep. Fail Trb. [9417].
2. Select Enabled or Disabled.

9.18: Cancel Alarm

The Cancel Alarm feature is an option that allows the user to cancel a false alarm by disarming the system within five minutes of reporting the alarm. Cancelling an alarm causes the control panel to report a Cancel event to the monitoring station and an enter an Alarm Cancelled event in the event log. Following a cancelled alarm, the message ***Alarm Cancelled***, ***OK?*** appears on the keypads' LCD until the user presses ✓ to confirm. Until confirmation is received, the control panel does not allow any local function to be performed. However, the control panel may perform remote commands received via Telecontrol or Remote Programming regardless of this system status. Please note that alarm indication has higher priority and overrides the "Alarm Cancelled" display.

As this control panel has been designed to meet the requirements of the ANSI/SIA CP-01 standard for false alarm reduction, it is not possible to disable the Cancel Alarm feature. Consequently, the system will reject any attempt to change the default setting of the menu item System Options, Cancel Alarm [9418].

© MARMITEK

9.19: Cross Zoning (for future use)

Cross Zoning is a future option that is not available in the current firmware. The default setting for this option is disabled. Marmitek recommends that you do not change this setting.

9.20: Verified Fire

The Verified Fire feature is an option that is designed to delay Fire alarm reports to the monitoring station until the alarm condition has been verified. Local Fire alarm indication is not affected by this option and the control panel shall sound the siren instantly on receiving an alarm from a smoke detector. You can program a Verified Fire timeout of between 00 and 60 seconds (00 = disabled).

If the Verified Fire feature is enabled, a Fire alarm event shall be reported if…

- An alarm occurs from a Fire zone and the alarm has not been restored by the end of the Verified Fire timeout – in this case, the alarm is reported at the end of the Verified Fire timeout.
- An alarm occurs from a Fire zone, the alarm is restored and then a second alarm occurs from the same zone during the Verified Fire timeout – in this case, the alarm is reported immediately on receiving the second alarm.
- An alarm occurs from a Fire zone and a second alarm occurs from an additional fire zone within the Verified Fire timeout – in this case, the alarm is reported immediately on receiving the second alarm.

To program the Verified Fire timeout:

1. From the Programming menu, select System Options, Verified Fire [9420].
2. Enter a value between 00 and 60 seconds (00 = disabled).
3. Press ✓ when the desired setting is displayed.

9.21: Battery Type

The battery type shall be defined according to the battery supplied with the system (for example, if the battery sticker reads 1500 mAh, choose 1.5 Ah, if 3000 mAh, choose 3.0 Ah)

To program the battery type:

1. From the Programming menu, select System Options, Battery Type [9421].
2. Select the battery type.
3. Press ✓ when the desired setting is displayed.

Chapter Ten: Communications

This section explains how to determine the way the control panel communicates via the GSM and PSTN modules.

10.1: Monitoring station Reporting

The control panel supports three customer accounts for monitoring station reporting. Each account has its own telephone number and communications options. An explanation of each of these options is included in this section.

10.1.1: Telephone Number

To edit an account's telephone number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Phone Number [#1].
4. Enter up to 16 digits. Use the key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialling), "P" (switch to pulse dialling) or "+" (international code). Use the key to delete one character at a time.
5. Press ✓ when you have finished editing.

10.1.2: Account Number

To edit an account number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Account Number [#2].
4. Enter up to eight digits. Enter leading zeros for account numbers of less than eight digits. Use the key to enter hexadecimal digits.

If the programmed protocol is Contact ID, "A" is not a valid entry in the account number.

5. Press ✓ when you have finished editing.

10.1.3: Protocol

To program an account's communication protocol:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Protocol [#3].
4. Select a protocol from the options available.

Account number 3 is designed for use with the Follow me feature. It is the only telephone number that can be programmed by the user.

10.1.4: Communication Interface

For each account, you can choose whether the system employs cellular or PSTN communication.

To program an account's communication interface:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Interface [#4].
4. Select either GSM or PSTN.

© MARMITEK

10.1.5: Call Attempts

The Call Attempts option determines the number of times the system tries to call a telephone number before moving on to the next number in sequence.

To program the number of call attempts for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Call Attempts [#5].
4. Enter a value between 01 and 15.
5. Press ✓ when the desired setting is displayed.

10.1.6: Two-Way Audio

The Two-Way audio option determines whether Two-Way Audio is enabled for the account. For further information, see section *5.2.2: TWA Alarm Reporting*.

To program the Two-Way Audio option for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (1-3).
3. From the account's sub-menu, select Two-Way Audio [#6].
4. Select Enabled or Disabled.

10.2: General Options for Monitoring station Reporting

The options included in this section concern the three accounts used for monitoring station reporting.

10.2.1: Call Continue

When reporting an event, the system attempts to call Telephone #1. If the system fails in its attempt to report the event, it dials Telephone #2 then Telephone #3, respectively. If the Call Continue feature is active, the control panel sends a duplicate report to the accounts that are selected. For example, using this feature, the system can send an alarm report to the monitoring station then notify the user by sending an SMS message to their mobile phone.

To program the Call Continue option:

1. From the Programming menu, select Communications, Accounts, Call Continue [9517]; the current Call Continue setting is displayed.

Press…	To…
1	Toggle Account #1 in the Call Continue sequence.
2	Toggle Account #2 in the Call Continue sequence.
3	Toggle Account #3 in the Call Continue sequence.

Table 10.1: Call Continue Options

2. Use keys 1, 2 and 3 to toggle the account numbers.
3. Press ✓ when the desired setting is displayed.

10.2.2: Report Cycles

The system's attempts to report events are organized in cycles. A report cycle is a set of call attempts. If the system does not succeed in sending a report to any of the telephone numbers, it tries to dial the entire report cycle again until it sends a successful report. You can determine the number of times the system attempts to dial this sequence by programming the Report Cycle option.

To program the number of Report Cycles:

1. From the Programming menu, select Communications, Accounts, Report Cycles [9518].
2. Enter a value between 01 and 03.
3. Press ✓ when the desired setting is displayed.

In the example illustrated in Figure 10.1, Account 1 is programmed with 2 call attempts, Account 2 is programmed with 3 call attempts and the number of report cycles programmed is 3.

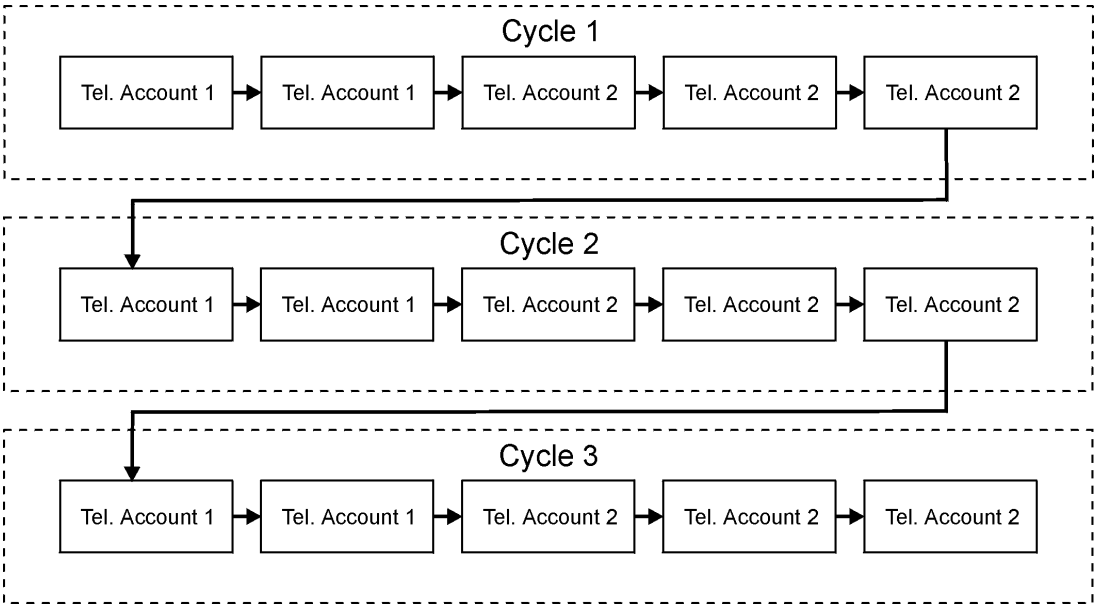


Figure 10.1: Typical Report Cycle Sequence

10.3: Vocal Message Dialler

The Vocal Message Dialler is a feature that calls the user's telephone number when specific events occur and plays pre-recorded messages. These calls are made after the system has reported the events to the monitoring station. Additionally, in the event of an alarm, the user is able to establish a Two-Way Audio connection on receiving the vocal message in order to check the premises.

The system supports three Vocal Message (VM) accounts. Each account has its own telephone number, communication interface and Two-Way Audio options.

The types of event that are reported using the Vocal Message Dialler feature are determined in VM Event Options – *see 10.10: Vocal Message Dialler Event Options*. If one of these events occurs, the control panel dials the phone number for VM Account 1.

The availability of the Vocal Message Dialler feature is hardware dependent.

© MARMITEK

The sequence for a vocal message call is as follows:

1. An event occurs and the control panel calls the telephone number of VM Account 1.
2. When the user answers the call, the Home ID message and the relevant event message are played.
3. The user presses 1 on their telephone; if there are additional events to report the next message is played. Otherwise, “No Further Messages” is announced.

   -or-

   If Two-Way Audio is enabled for the VM account, the user may open the audio channel by pressing 2 on their telephone. If the user does not want to open the audio channel they may press “*” then “#” on their telephone to hang up.

The Vocal Message Dialler feature implements 3 call cycles when attempting to call the Vocal Message (VM) accounts.

If a call to VM account 1 is not answered or the TC/VM Timeout (see *10.6.11: Telecontrol/Vocal Message Timeout*) expires before the message is acknowledged by the user pressing 1, the control panel calls the telephone number programmed for VM Account 2 then VM account 3.

If none of the calls are acknowledged, this cycle is repeated twice.

This means that the control panel performs a maximum of three call attempts to each VM account.

10.3.1: Telephone Number

To edit a Vocal Message account’s telephone number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a VM account (4-6).
3. From the account’s sub-menu, select Phone Number [#1].
4. Enter up to 16 digits. Use the key to enter “*”, “#”, “,” (pause), “T” (switch to DTMF tone dialling), “P” (switch to pulse dialling) or “+” (international code). Use the key to delete one character at a time.
5. Press ✓ when you have finished editing.

10.3.2: Communication Interface

For each Vocal Message account, you can choose whether the system employs cellular or PSTN communication.

To program a Vocal Message account’s communication interface:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a VM account (4-6).
3. From the account’s sub-menu, select Interface [#2].
4. Select either GSM or PSTN.

10.3.3: Two-Way Audio

The Two-Way audio option determines whether Two-Way Audio is enabled for the Vocal Message account. For further information, see section *5.2.3: Two-Way Audio after Vocal Messages.*

To program the Two-Way Audio option for a VM account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select a CS account (4-6).
3. From the account's sub-menu, select Two-Way Audio [#3].
5. Select Enabled or Disabled.

10.3.4: Home ID

The Home ID is a short message that is played at the beginning of a vocal message call in order to identify the system to the user. For example, at the beginning of the vocal message call, the message "Michael's House" shall be played before the event messages.

To play back the Home ID message:

- From the Programming menu, select Communications, Accounts, Home ID, Play Message [95191].

To record a Home ID message:

1. From the Programming menu, select Communications, Accounts, Home ID, Record Message [95192].
2. Press ✓ to start recording the message.
3. Record your message. The message may be up to ten seconds long.
4. Press ✓ to stop recording; the message is automatically played back and OK? is displayed.
5. Press ✓ to save your recording.

10.4: Remote Programming

Marmitek's ProGuard800 Remote Programmer (RP) software enables you to operate and program the system from a PC either on-site or from a remote location. The software provides a comprehensive interface to the *ProGuard800* control panel designed to facilitate programming.

You can connect to the panel from a PC using one of three methods:

- Direct Call: The RP calls the site, the system picks up and RP communication is established.
- Call-back: The RP calls the site, the system picks up then hangs up. The system then calls the Call-back telephone number to establish a connection.
- USB Connection: The RP connects directly via the Main board's USB port (this method requires that you buy a USB Interface).

The following programming options relate to the method in which the Remote Programmer software connects with the system.

10.4.1: Call-back Telephone Number

RP Call-back is a security feature that helps ensure that remote programming is only performed by authorized personnel. When the Remote Programmer contacts the panel, the panel hangs up and calls the Call-back telephone number.

© MARMITEK

To edit the Call-back telephone number:

1. From the Programming menu, select Communications, Remote Prog., Call-Back # [9521].
2. Enter up to 16 digits. Use the key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialling), "P" (switch to pulse dialling) or "+" (international code). Use the key to delete one character at a time.
3. Press ✓ when you have finished editing.

If there is no Call-back telephone number programmed, RP Call-back is disabled and the system connects to the Remote Programmer software using the "direct call" method.

10.4.2: RP Pass code

The RP pass code is a six-digit code that grants access to remote programming. When establishing an RP connection, the pass code programmed in the RP customer file on the PC must be identical to the system's RP pass code.

To edit the RP pass code:

1. From the Programming menu, select Communications, Remote Prog., RP Passcode [9522].
2. Enter six digits.
3. Press ✓ when you have finished editing.

10.4.3: RP Communication Interface

The *ProGuard800* can employ either cellular or PSTN communication during remote programming.

For PSTN communication, the RP uses a double call method so that the line can be shared with regular telephone handsets, an answering machine or fax. The Cellular Communications Module has its own individual telephone number for data transfer and therefore, the double call method is not needed. In this case, the RP calls the control panel directly.

To program the RP communication interface:

1. From the Programming menu, select Communications, Remote Prog., RP Interface [9523].
2. Select either GSM or PSTN.

10.4.4: RP Access Options

Options are available to enable, disable or limit access to remote programming.

To program RP Access Options:

1. From the Programming menu, select Communications, Remote Prog., RP Access [9524].
2. Select an RP access option from the following table.

Access option	Description
Always Enable	Up/downloading is always possible.
During Disarm	The system must be disarmed in order to establish a connection.
Disable	Up/downloading is disabled.
User Initiated	The user must perform Enable Programming from the Service menu in order to establish a connection – *see 4.7.11: Enable Programming.*

Table 10.2: RP Access Options

10.5: Service Call

The Service Call feature is designed to enable the user to call the monitoring service at the push of a button. When the user presses and holds down the Service Call button (0) for a few seconds, a two-way audio connection is established with the monitoring station.

10.5.1: Service Call Telephone Number

To edit the Service Call telephone number:

1. From the Programming menu, select Communications, Service Call, Phone Number [9531].
2. Enter up to 16 digits. Use the key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialling), "P" (switch to pulse dialling) or "+" (international code). Use the key to delete one character at a time.
3. Press ✓ when you have finished editing.

10.5.2: Service Call Interface

For the Service Call feature, you can choose whether the system employs cellular or PSTN communication.

To program the Service Call interface:

1. From the Programming menu, select Communications, Service Call, Interface [9532].
2. Select either GSM or PSTN.

10.6: Communications Options

10.6.1: Line Monitor

The Line Monitor feature monitors both the PSTN telephone line and the GSM network. If a problem is detected with either of these, a Media Loss event is registered in the log.

To program the Line Monitor setting:

1. From the Programming menu, select Communications, Comm. Options, Line Monitor [95401].
2. Select Enabled or Disabled.

10.6.2: Periodic Test Interval

The Periodic Test is a test transmission the system sends to notify the monitoring station that its reporting capability is fully functional.

Two options are available for the Periodic Test:

- You can program the system to send a Periodic Test message according to a chosen time interval. This time interval can be between 1 and 254 hours (approximately 10 days).
- The system calculates automatically the time the Periodic Test is sent according to the last four digits of the account number. Automatically calculated tests can be sent daily, weekly or monthly according to the Auto Interval option – *see 10.6.4: Auto Interval*. This feature ensures that the monitoring station is not inundated by test reports at any given time.

© MARMITEK

The Periodic Test event message is an unclassified event. This means that it does not belong to any event group. If the Periodic Test Interval is programmed with any value other than 000, the event message shall be sent.

To program the Periodic Test Interval:

1. From the Programming menu, select Communications, Comm. Options, Test Interval [95402].
2. Enter the test interval (001-254 hours) or 255 for an automatically calculated test interval.
3. Press ✓ when the desired setting is displayed.

To disable the Periodic Test:

- Program the Periodic Test Interval as 000.

10.6.3: First Test

If the Periodic Test Interval is programmed as 001-254 hours, you must also program the time that the first Periodic Test is sent.

To program the First Test Time:

1. From the Programming menu, select Communications, Comm. Options, First Test [95403].
2. Enter a time (HH:MM).
3. Press ✓ when the desired setting is displayed.

10.6.4: Auto Interval

The Auto Interval option determines the frequency of automatically calculated periodic test messages.

To program the Auto Interval:

1. From the Programming menu, select Communications, Comm. Options, Auto Interval [95404].
2. Select Daily, Weekly or Monthly.

10.6.5: Call Timeout

The Call Timeout is the amount of time the system waits for the first acknowledgement (ACK1) from the monitoring station when reporting using the PSTN module. If ACK1 is not received during this time, the system regards the call as a failed dialing attempt.

To program the Call Timeout:

1. From the Programming menu, select Communications, Comm. Options, Call Timeout [95405].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

10.6.6: ACK. Timeout

The ACK Timeout is the amount of time the system waits for the second acknowledgement (ACK2) from the monitoring station when reporting using the PSTN module. If ACK2 is not received during this time, the system regards the call as a failed dialing attempt.

To program the ACK Timeout:

1. From the Programming menu, select Communications, Comm. Options, ACK Timeout [95406].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

10.6.7: PSTN Country

In order to meet the requirements of local telecommunications authorities, default telephone line parameters have been chosen for a number of different countries.

To program the PSTN Country:

1. From the Programming menu, select Communications, Comm. Options, PSTN Country [95407].
2. Select your country from the options available.

Marmitek offers custom telephone line parameter settings for countries that do not appear in the list of pre-defined options. If your country does not appear among the available options, select the option Custom Settings.

10.6.8: Dial Tone Wait

This option determines whether the system dials only when the dial tone is present or if the dialling is initiated regardless of the dial tone.

To program the Dial Tone Wait option:

1. From the Programming menu, select Communications, Comm. Options, Dial Tone Wait [95408].
2. Select Enabled or Disabled.

10.6.9: RDM Period

Remote Diagnostics and Maintenance (RDM) session is a feature that is designed to enable automated maintenance of installed control panels. During a maintenance session, the control panel automatically dials the RP Call-back number and connects to the RDM server. The time interval between maintenance sessions is called the RDM period.

To program the RDM period:

1. From the Programming menu, select Communications, Comm. Options, RDM Period [95409].
2. Enter the required RDM period (001-255 days or 000 to disable RDM communication).
3. Press ✓ when the desired setting is displayed.

10.6.10: Incoming Calls

This option determines whether the panel is able to receive incoming Telecontrol/Two-Way Audio calls.

To program the Incoming Calls option:

1. From the Programming menu, select Communications, Comm. Options, Incoming Call [95410].
2. Select Enabled or Disabled.

10.6.11: Telecontrol/Vocal Message Timeout

The Telecontrol/Vocal Message Timeout (TC/VM Timeout) determines the duration of a Telecontrol, Two-Way Audio or Vocal Message call. In the case of a Telecontrol or Two-Way Audio call, when the time out expires, the system automatically disconnects unless the call is manually extended by the operator. For Vocal Message calls, if the time out expires and the user has not acknowledged the message, the system attempts to call the next VM account's telephone number. During a Vocal Message call, the timeout is reset each time a message is acknowledged.

© MARMITEK

To program the Telecontrol/Vocal Message Timeout:

1. From the Programming menu, select Communications, Comm. Options, TC/VM Timeout [95411].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

10.6.12: TWA Mode

The Two-Way audio features offer a choice of two operation modes:

- Duplex – both parties may speak at once just like a regular telephone.
- Simplex – one party may speak while the other party listens.

To program the TWA mode option:

1. From the Programming menu, select Communications, Comm. Options, Two-Way Audio, TWA Mode [95412].
2. Select Duplex or Simplex.

10.7: GSM Options

10.7.1: GSM RX Report

The GSM RX Report is a feature that periodically reads the GSM signal strength of the Cellular Communications module – *see 4.7.9: GSM Signal Strength*. This reading occurs at the times programmed for the Periodic Test – *see 10.6.2: Periodic Test Interval & 10.6.3: First Test.* This means that each time the periodic test is sent, the system also sends a GSM signal strength report to the monitoring station. The system also enters the GSM signal strength in the event log.

If the Periodic Test is disabled, the GSM RX Report feature will not function.
The GSM RX report belongs to the Peripherals event group – see 10.9: Event Options for Monitoring station Reporting. If this event group is disabled, the GSM signal strength is still recorded in the event log.

To program the GSM RX Report option:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, GSM RX Report [954131].
2. Select Enabled or Disabled.

10.7.2: PIN Code

The PIN (Personal Identity Number) is a four-digit code that protects the SIM card from unauthorized use if lost or stolen.

To program the PIN code:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, PIN Code [954132].
2. Edit the four-digit PIN code.
3. Press ✓ when you have finished editing.

10.7.3: SMS Center

To edit the SMS Centre telephone number:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Center [954133].
2. Enter up to 16 digits. Use the 💡 key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialling), "P" (switch to pulse dialling) or "+" (international code). Use the 💡 key to delete one character at a time.
3. Press ✓ when you have finished editing.

10.7.4: SMS Command

The SMS Command option enables you to enable or disable the ability to send commands to the system via SMS. For further information on SMS commands, *see 3.8: Remote Arming/Disarming via SMS* and *6.3: Telephone Control*

To enable/disable SMS commands:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Command [954134].
2. Select Enabled or Disabled.

10.7.5: SMS Confirmation

After an SMS command is executed by the system, a confirmation message is returned to the sender's mobile phone. You can enable or disable this feature using this option.

To enable/disable SMS confirmation:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Confirm. [954135].
2. Select Enabled or Disabled.

10.7.6: GSM Media Loss Time

The GSM Media Loss Time is a feature that is designed to reduce the amount of GSM media loss events registered in the log and sent to the monitoring station. This feature is recommended for use in cases of wide fluctuation of GSM signal strength.

If a problem is detected with the GSM, a Media Loss event is registered in the log and sent to the monitoring station after the time defined in the GSM ML Time parameter.

GSM Media Restore will be registered in the log and sent to monitoring station always 3 minutes after GSM media restore is detected.

This feature is implemented only when the Line Monitor feature is enabled (*see 10.6.1 Line Monitor*).

To disable the GSM Media Loss feature (cancel the GSM Media Loss events) enter 000.

To program the GSM Media Loss Time:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, GSM ML Time. [954136].
2. Enter time (003-255 minutes or 000 to disable).
3. Press ✓ when the desired setting is displayed.

10.8: TWA Event Report Options

10.8.1: TWA Event Report

The TWA Event Report is an event report that is sent to the monitoring station to indicate that Two-Way Audio communication is about to commence. If enabled, the system sends the Contact ID event code 606000 before establishing Two-Way Audio communication.

This option affects Contact ID only. If using SIA, a TWA event report is always sent together with the TC/VM timeout, regardless of the configuration for this option.

© MARMITEK

To program the TWA Event option:

1. From the Programming menu, select Communications, Comm. Options, TWA Event Rept. [95414].
2. Select Enabled or Disabled.

10.8.2: TWA Time Report

If the TWA Time Report option is enabled, the last three digits of the TWA Event Report are replaced with the amount of seconds programmed for the TC/VM Timeout – *see 10.6.11: Telecontrol/Vocal Message Timeout*. For example, if the TC/VM Timeout is programmed as 120 seconds, the Contact ID event code that shall be sent for the TWA Event Report shall be 606120.

To program the TWA Time Report option:

1. From the Programming menu, select Communications, Comm. Options, TWA Time Rept. [95415].
2. Select Enabled or Disabled.

10.9: Event Options for Monitoring station Reporting

System events are divided into a number of different event groups. This division allows you to enable or disable reporting or Two-Way Audio for a specific group of events.

The different event groups are as follows:

- Burglary [#1]
- Fire [#2]
- Open/Close (arm/disarm) [#3]
- Service [#4]
- Power [#5]
- Peripherals [#6]
- RF Jamming [#7]
- Medical [#8]

10.9.1: Event Reporting

You can enable or disable event reporting per Event Group. This allows you to filter the type of events that are reported to the monitoring station.

To enable/disable reporting for an event group:

1. From the Programming menu, select Communications, Event Options [955].
2. Select an Event Group.
3. From the event group's sub-menu, select Report [#1].
4. Select Enabled or Disabled.

10.9.2: Restore Reporting

For each event group, you can determine whether restore messages shall be sent.

To enable/disable restore reporting for an event group.

1. From the Programming menu, select Communications, Event Options [955].
2. Select an event group.
3. From the event group's sub-menu, select Report Restore [#2].

4. Select Enabled or Disabled.

10.9.3: Two-Way Audio

For Burglary, Fire and Medical event groups, there is an additional option that enables Two-Way Audio for that event group – *see 5.2.2: TWA Alarm Reporting.*

To enable/disable Two-Way Audio for an event group:

1. From the Programming menu, select Communications, Event Options [955].
2. Select an Event Group (Burglary, Fire or Medical).
3. Select TWA [#3].
4. Select Enabled or Disabled.

10.10: Vocal Message Dialler Event Options

Events reported using the Vocal Message Dialler are divided into event groups that correspond with the pre-recorded event messages. This allows you to enable or disable the Vocal Message feature for a specific group of events. For further information on this feature, see *10.3: Vocal Message* .

The vocal message event groups and their associated system events are as follows:

- Burglary [#1]
  - Alarm from Zone (excluding Gas, Flood and Environmental zones)
  - Zone Tamper
  - Tamper
  - Duress
- Fire [#2]
  - Zone Fire Alarm
  - User Activated Fire Alarm
- Panic [#3]
  - Zone Panic Alarm
  - User Activated Panic Alarm
- Medical [#4]
  - Zone Medical Alarm
  - User Activated Medical Alarm
  - No Motion
- System Trouble [#5]
  - Battery Low
  - Transmitter Low Battery
  - AC Loss
  - Media Loss
  - Device Trouble
  - Communication Trouble
  - Transmitter Out of Synch.
  - Control Panel Transmitter Out of Synch.
  - Supervision Loss
  - Zone Trouble
  - FM Jamming

© MARMITEK

- Arm [#6]
  - Full Arm
  - Part Arm
  - Perimeter Arm
- Disarm [#7]
  - Disarm
  - Disarm after Alarm
- Water [#8]
  - Zone Water Alarm (Flood)

To enable/disable the vocal message for an event group:

1. From the Programming menu, select Communications, VM Event Opt. [956].
2. Select an event group.
3. Select Enabled or Disabled.

Chapter Eleven: X-10 Home Automation Programming

This chapter explains the programmable options for the system's home automation features. The Home Automation module is an add-on optional extra that you can install inside the panel's plastic housing.

11.1: X-10 Overview

The control panel's home automation feature employs the X-10 protocol and this enables compatibility with a wide variety of readily available home automation products.

Before you can start programming the system's Home Automation features, you should be familiar with the basic concept behind X-10 automation.

X-10 is a protocol that enables you to send commands and other data over regular existing power lines. This means that, using an X-10 transmitter (the panel's Home Automation module), you can send On/Off commands to X-10 receivers (lamp and appliance modules) that are plugged into electricity outlets around the home. From here on, we shall refer to these X-10 receivers as "HA units".

Each HA unit has two codes that are used for identification. These codes are known as the House code and the Unit code and are usually defined by adjusting the dials that appear on the X-10 unit. In Figure 11.1, the HA unit is set to House A, Unit 3.

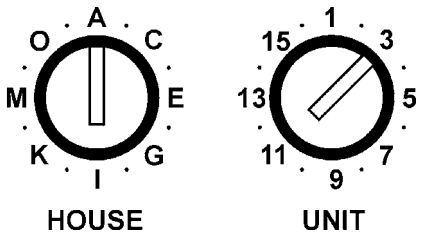


Figure 11.1: HA Unit Dials

The control panel supports sixteen HA units on one House code. To ensure that the Home Automation features function correctly, you must abide by the following guidelines.

- The House code must be the same on each HA unit.
- The House code on the HA units must be identical to the House code programmed in the panel's memory – *see section 11.3: House Code.*

11.2: HA Units

The following sections explain the programming options available for HA units.

11.2.1: Scheduling

Scheduling allows you to program the panel to send On/Off commands to an HA unit at specific times. The Scheduling section of Home Automation programming is identical to that described in Chapter Six: X-10 Home Automation Control. For further information on programming the On Time, Off Time and Schedule for each HA unit, see section *6.4:* Scheduling.

© MARMITEK

11.2.2: On by Zone

The On by Zone feature allows you to choose two zones that activate the HA unit when triggered. When either one of these zones is triggered, the system sends an On command to the HA unit according to the unit's programmed Pulse Time – *see 11.2.8: Pulse Time*. For example, you have a magnetic contact installed above the front door. When the door is opened, the hall light is lit.

To select the sensors that activate an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Zone [#04].
4. Enter up to two zone numbers.
5. Press ✓ when the desired setting is displayed.

11.2.3: On by Arm

The On by Arm feature activates the HA unit when the system is armed using any of the arming methods. The amount of time the HA unit is activated is determined by the Pulse Time – *see 11.2.8: Pulse Time*. If the Pulse Time is programmed as "Toggle", disarming the system switches the HA unit off.

To program the On by Arm feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Arm [#05].
4. Select Enabled or Disabled.

11.2.4: On by Alarm

On by Alarm is a feature designed for use with X-10 sirens. When an alarm occurs, the HA unit (i.e. siren) is activated for the duration of the siren cutoff – *see 7.10.3: Siren Cut-Off*. The X-10 siren sounds a continuous pattern for intrusion/panic alarms and a pulsed pattern for fire alarms.

To program the On by Alarm feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Alarm [#06].
4. Select Enabled or Disabled.

If an HA unit is programmed to be activated by the On by Alarm feature, program all other operation modes (On by Arm, Randomize, etc.) as disabled.

Do not program more than one HA unit to be activated by the On by Alarm feature. If more than one siren is required, set all sirens with the same House and Unit code.

11.2.5: Keyfob Control

Each KR814 Keyfob, offers control of up to two individual HA units. This programming option allows you to enable or disable this feature per HA unit.

To program the Keyfob control option for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].

2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select KF Ctrl [#07].
4. Select Enabled or Disabled.

11.2.6: Telephone Control

Via SMS or DTMF, you can send commands to the system in order to control various HA units. This option allows you to enable or disable this feature for each HA unit.

To program the SMS control option for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select TEL CTRL [#08]. [#08].
4. Select Enabled or Disabled.

11.2.7: Randomize

When the system is fully armed between the hours 9:00pm and 6:00am, the Randomize feature turns HA units on and off at random. This gives the impression that the house is occupied and acts as a deterrent against potential intruders.

To program an HA unit to be included in the Randomize feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Randomize [#09].
4. Select Enabled or Disabled.

11.2.8: Pulse Time

The Pulse Time determines the manner in which an HA unit responds to the On command. You can program each HA unit switch on momentarily. This means that, on receiving the On command, the unit will be switched on for a programmed amount of time. For example, you can program the hall light to switch on for 1 minute and automatically switch itself off. Alternatively, the HA unit can be programmed to toggle on and off.

To program the Pulse Time for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Pulse Time [#10].
4. Select 5 sec, 30 sec, 1 min, 2 min or Toggle.

11.2.9: Descriptor

You can assign a 16-character descriptor for each HA unit. These descriptors help the user to identify the various HA units installed around the home.

To edit an HA unit descriptor:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Descriptor [#11].
4. Edit the descriptor using the alphanumeric keypad.
5. Press ✓ when you have finished editing.

© MARMITEK

11.3: House Code

The House code is part of the identification code of each HA unit. For the Home Automation features to function correctly, the House code on each HA unit must be identical to the House code programmed in the system's memory.

To program the system House code:

1. From the Programming menu, select HA Programming, House Code [962].
2. Using the arrow keys, select a House code from the options available (A-P).

11.4: HA Control

The HA Control option allows you to enable or disable all Home Automation features for the entire system.

To program the Home Automation setting:

1. From the Programming menu, select System Options, HA Control [963].
2. Select Enabled or Disabled.

Chapter Twelve: System Initialization

The Initialization menu offers a number of options that enable you to reset the system. This menu is particularly useful when re-installing a panel at a new site. The Initialization function clears the entire system. This restores programming defaults, clears the log, user codes and the transmitter register. Options are also available that enable you to clear a specific section of the system's memory separately.

12.1: Initialization

The Initialization function clears the entire system and resets factory defaults. If your system does not include multi-default and multi-language support, skip steps 2 and 3 of the following procedure.

To initialize the control panel:

1. From the Programming menu, select Initialize, Init All [971]; the system prompts you for confirmation.
2. For firmware versions that include multi-default and multi-language support, select the set of programming defaults that you want to load.
3. For firmware versions that include multi-default and multi-language support, select the required interface language.
4. Press ✓ to confirm; factory programming defaults are restored, the event log is cleared, user codes and wireless transmitters are deleted.

During system initialization, recorded vocal messages (Message Centre and Home ID) are not deleted.

12.2: Default Program Restore

Loading the system's default program enables you to restore the factory-set programming defaults.

To load the default program:

1. From the Programming menu, select Initialize, Load Defaults [972]; the system prompts you for confirmation.
2. Press ✓ to confirm; factory programming defaults are restored.

12.3: Clear User Codes

Clear User Codes deletes all programmed user codes and restores the default Master and Installer codes.

To clear user codes:

1. From the Programming menu, select Initialize, Clear Users [973]; the system prompts you for confirmation.
2. Press ✓ to confirm; all user codes are deleted and default codes are restored.

© MARMITEK

12.4: Clear Wireless Transmitters

The Clear Wireless Transmitters function enables you to delete all registered transmitters at once.

To clear the transmitter register:

1. From the Programming menu, select Initialize, Clear Wireless [974]; the system prompts you for confirmation.
2. Press ✓ to confirm; the transmitter register is cleared.

12.5: Find Modules

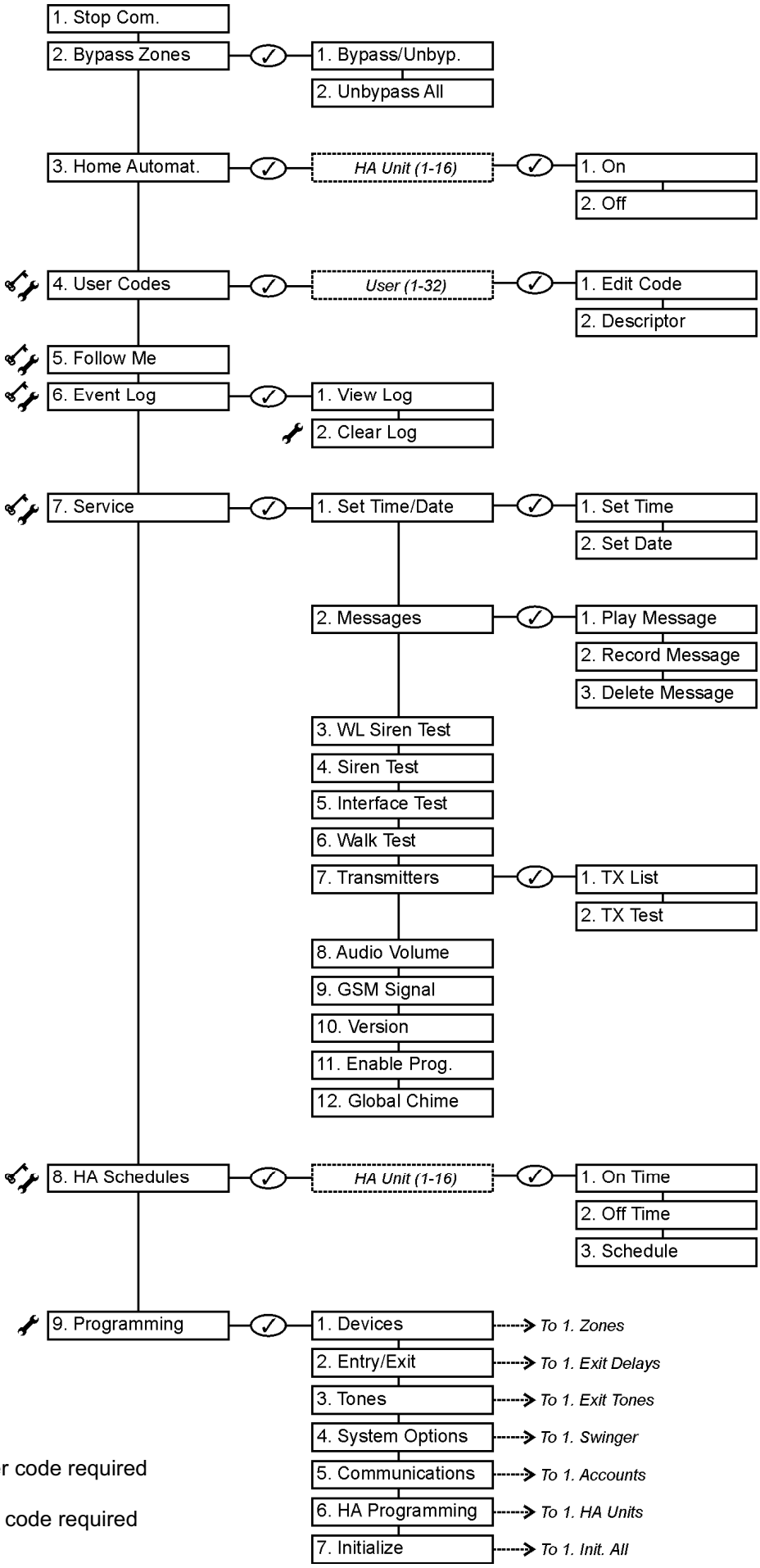
The Find Modules function runs a diagnostic test that identifies the modules and keypads that are connected to the system bus. With this information, the system knows which add-on modules should be present, enabling supervision for those modules.

To run the Find Modules test:

1. From the Programming menu, select Initialize, find Modules [975]; the system prompts you for confirmation.
2. Press ✓ to confirm; the system begins to search for the connected modules. At the end of the search, the modules that are present are displayed and the system asks if you want to save the displayed list.
3. Press ✓; the list is saved.

If a connected module is not included in the list, check the wiring connections and run this test again.

Appendix A: Menu Structure

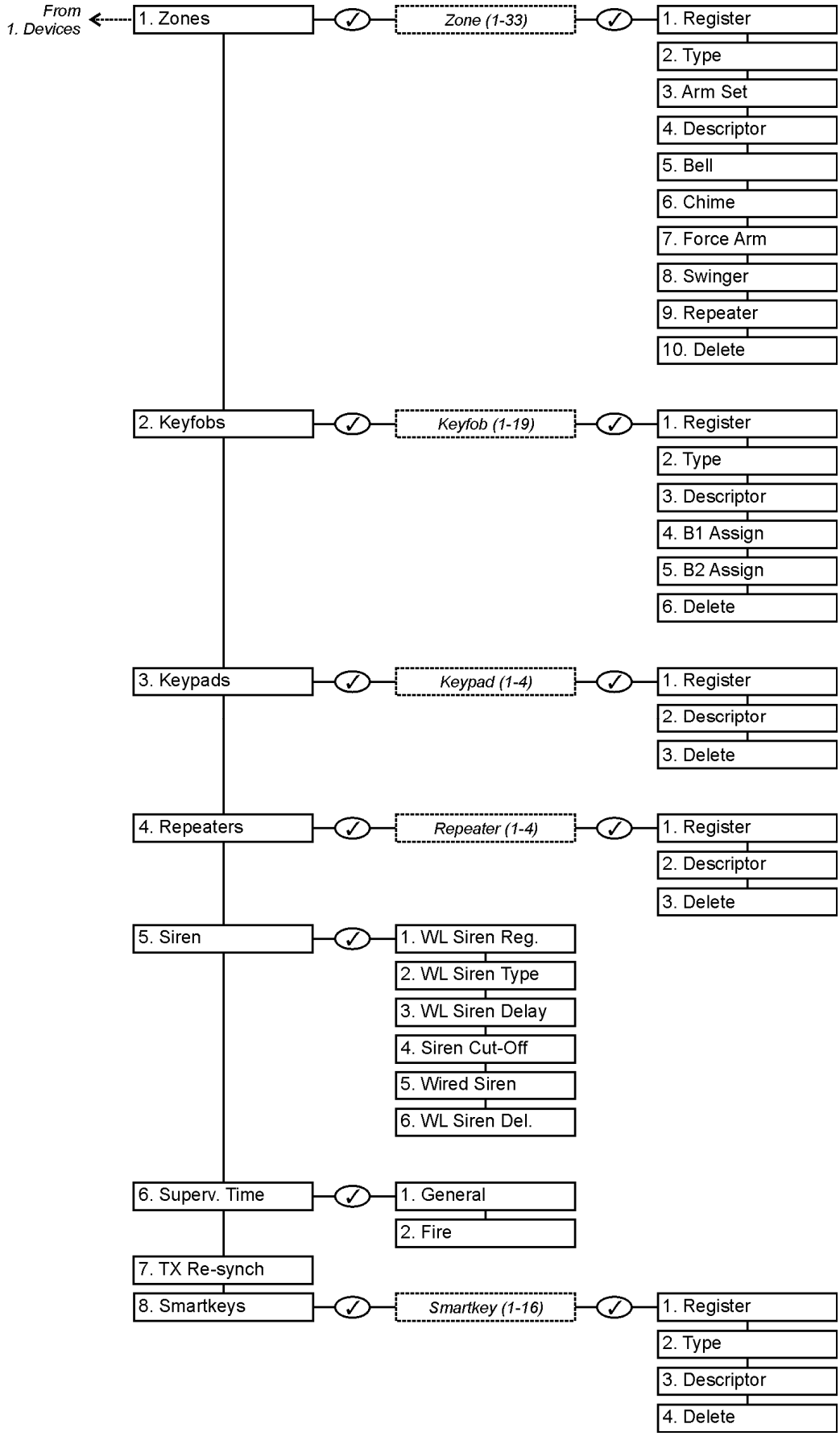


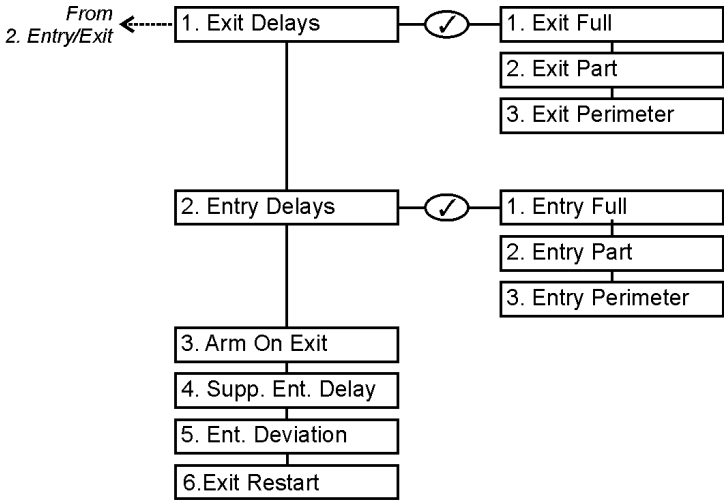
Legend:

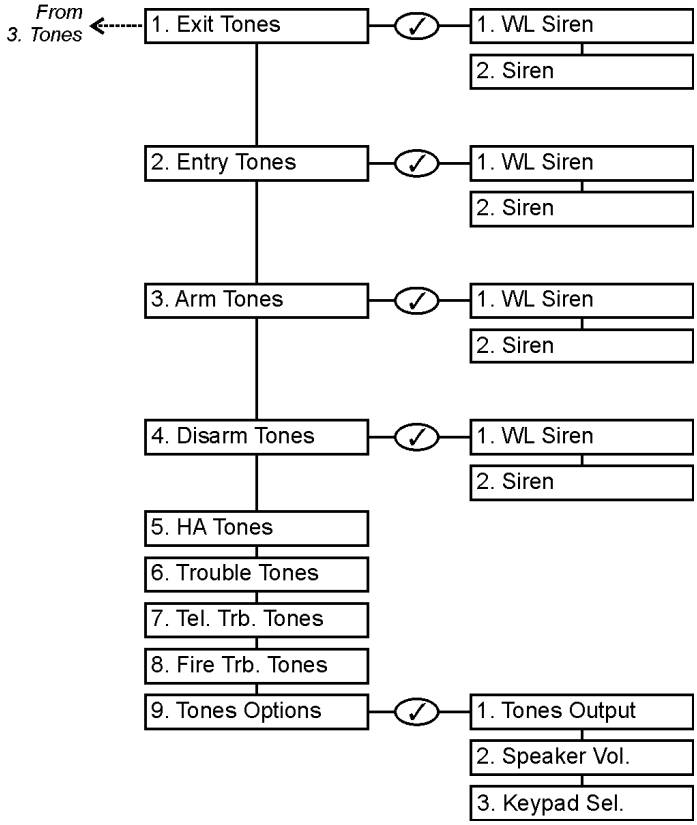
Installer code required

Master code required

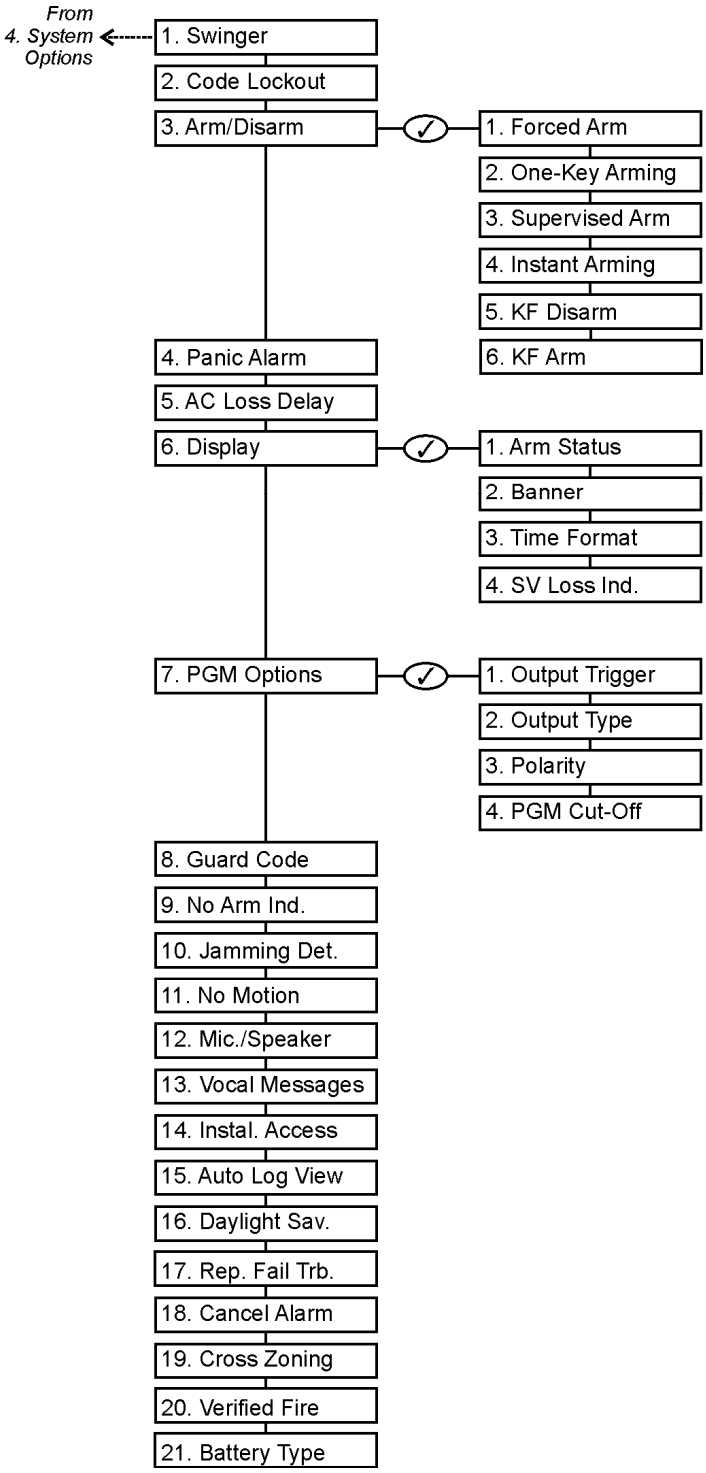
© MARMITEK

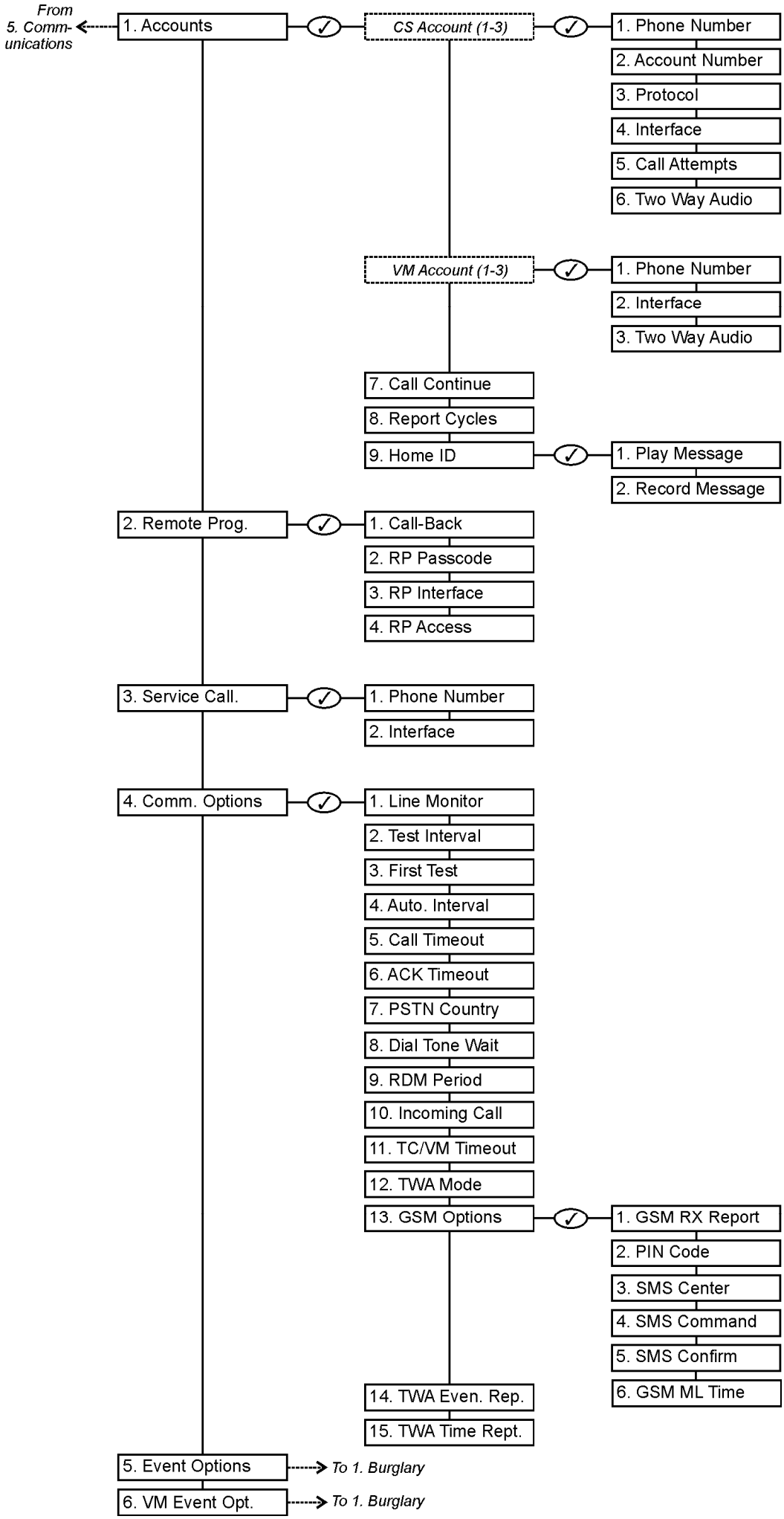

From
1. Devices
1. Zones
Zone (1-33)
1. Register
2. Type
3. Arm Set
4. Descriptor
5. Bell
6. Chime
7. Force Arm
8. Swinger
9. Repeater
10. Delete
2. Keyfobs
Keyfob (1-19)
1. Register
2. Type
3. Descriptor
4. B1 Assign
5. B2 Assign
6. Delete
3. Keypads
Keypad (1-4)
1. Register
2. Descriptor
3. Delete
4. Repeaters
Repeater (1-4)
1. Register
2. Descriptor
3. Delete
5. Siren
1. WL Siren Reg.
2. WL Siren Type
3. WL Siren Delay
4. Siren Cut-Off
5. Wired Siren
6. WL Siren Del.
6. Superv. Time
1. General
2. Fire
7. TX Re-synch
8. Smartkeys
Smartkey (1-16)
1. Register
2. Type
3. Descriptor
4. Delete


From
2. Entry/Exit
1. Exit Delays
1. Exit Full
2. Exit Part
3. Exit Perimeter
2. Entry Delays
1. Entry Full
2. Entry Part
3. Entry Perimeter
3. Arm On Exit
4. Supp. Ent. Delay
5. Ent. Deviation
6.Exit Restart

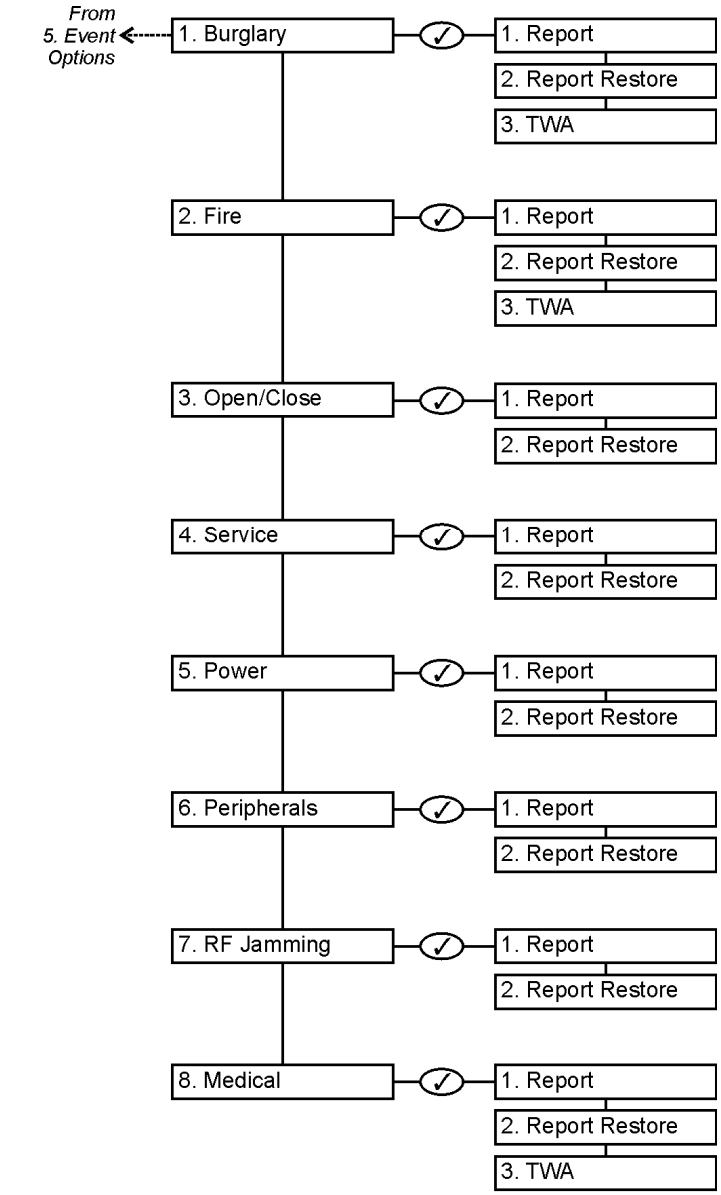

From
3. Tones
1. Exit Tones
1. WL Siren
2. Siren
2. Entry Tones
1. WL Siren
2. Siren
3. Arm Tones
1. WL Siren
2. Siren
4. Disarm Tones
1. WL Siren
2. Siren
5. HA Tones
6. Trouble Tones
7. Tel. Trb. Tones
8. Fire Trb. Tones
9. Tones Options
1. Tones Output
2. Speaker Vol.
3. Keypad Sel.

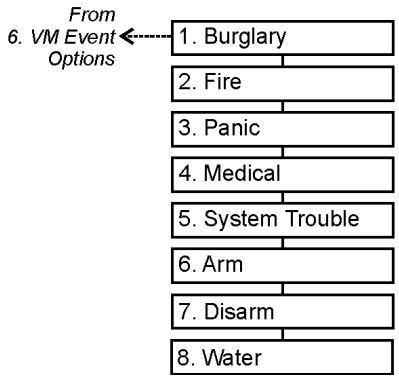
© MARMITEK

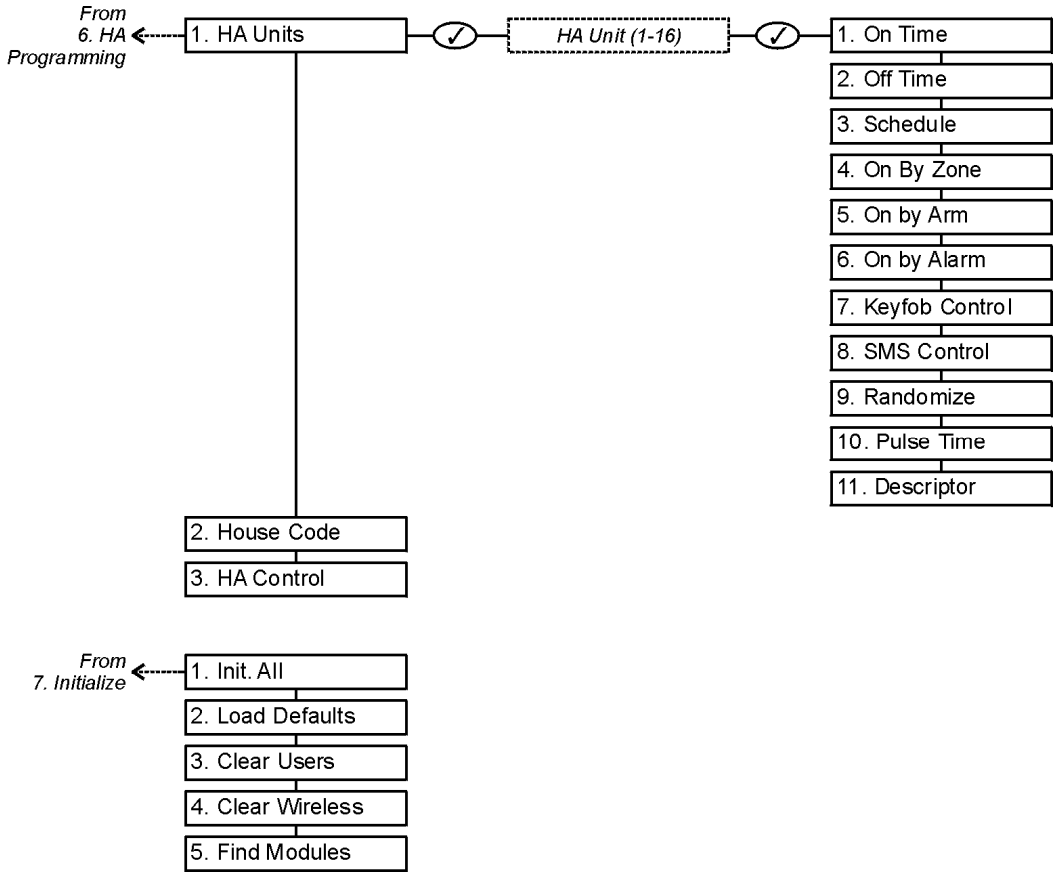

From
4. System
Options
1. Swinger
2. Code Lockout
3. Arm/Disarm
1. Forced Arm
2. One-Key Arming
3. Supervised Arm
4. Instant Arming
5. KF Disarm
6. KF Arm
4. Panic Alarm
5. AC Loss Delay
6. Display
1. Arm Status
2. Banner
3. Time Format
4. SV Loss Ind.
7. PGM Options
1. Output Trigger
2. Output Type
3. Polarity
4. PGM Cut-Off
8. Guard Code
9. No Arm Ind.
10. Jamming Det.
11. No Motion
12. Mic./Speaker
13. Vocal Messages
14. Instal. Access
15. Auto Log View
16. Daylight Sav.
17. Rep. Fail Trb.
18. Cancel Alarm
19. Cross Zoning
20. Verified Fire
21. Battery Type


From 5. Comm-unications
1. Accounts
CS Account (1-3)
1. Phone Number
2. Account Number
3. Protocol
4. Interface
5. Call Attempts
6. Two Way Audio
VM Account (1-3)
1. Phone Number
2. Interface
3. Two Way Audio
7. Call Continue
8. Report Cycles
9. Home ID
1. Play Message
2. Record Message
2. Remote Prog.
1. Call-Back
2. RP Passcode
3. RP Interface
4. RP Access
3. Service Call.
1. Phone Number
2. Interface
4. Comm. Options
1. Line Monitor
2. Test Interval
3. First Test
4. Auto. Interval
5. Call Timeout
6. ACK Timeout
7. PSTN Country
8. Dial Tone Wait
9. RDM Period
10. Incoming Call
11. TC/VM Timeout
12. TWA Mode
13. GSM Options
1. GSM RX Report
2. PIN Code
3. SMS Center
4. SMS Command
5. SMS Confirm
6. GSM ML Time
14. TWA Even. Rep.
15. TWA Time Rept.
5. Event Options
To 1. Burglary
6. VM Event Opt.
To 1. Burglary

© MARMITEK


From
5. Event
Options
1. Burglary
1. Report
2. Report Restore
3. TWA
2. Fire
1. Report
2. Report Restore
3. TWA
3. Open/Close
1. Report
2. Report Restore
4. Service
1. Report
2. Report Restore
5. Power
1. Report
2. Report Restore
6. Peripherals
1. Report
2. Report Restore
7. RF Jamming
1. Report
2. Report Restore
8. Medical
1. Report
2. Report Restore
3. TWA

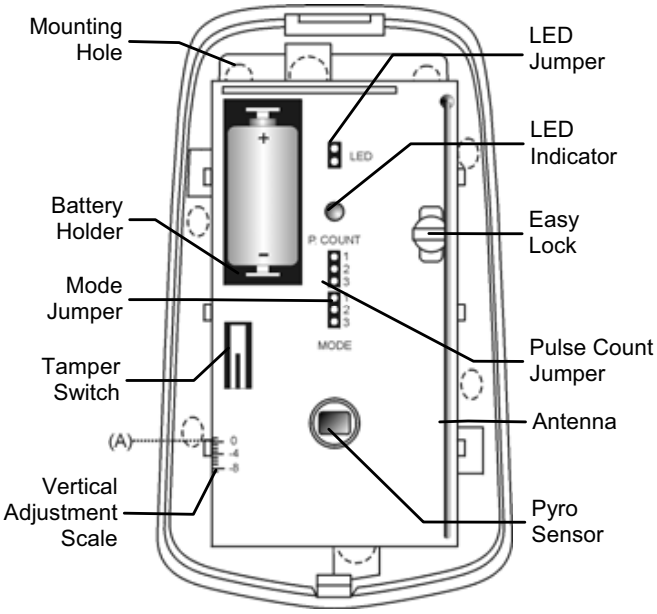

From
6. VM Event
Options
1. Burglary
2. Fire
3. Panic
4. Medical
5. System Trouble
6. Arm
7. Disarm
8. Water


From
6. HA
Programming
1. HA Units
HA Unit (1-16)
1. On Time
2. Off Time
3. Schedule
4. On By Zone
5. On by Arm
6. On by Alarm
7. Keyfob Control
8. SMS Control
9. Randomize
10. Pulse Time
11. Descriptor
2. House Code
3. HA Control
From
7. Initialize
1. Init. All
2. Load Defaults
3. Clear Users
4. Clear Wireless
5. Find Modules

© MARMITEK

PIR Sensors (MS845)

The MS845 are intelligent wireless PIR sensors for use with the *ProGuard800* system. All of these sensors implement a feature to combat the problem of multiple transmissions, which drastically reduce the life of the batteries. After each transmission, there is a four-minute delay during which further transmissions will not be sent.
The MS845 are designed for installations prone to nuisance alarms caused by pets or small animals.



Considerations Before Installation

- Select a location from which the pattern of the detector is most likely to be crossed by a burglar, should there be a break in.
- Do not place bulky objects in front of the detector.
- Avoid a location which comes in direct contact with radiators, heating/cooling ducts, mirrors and air conditioners.
- Select an appropriate installation height from Table B1.

Lens	Mounting Height
Standard	2.2m (6.6')
Long Range	2m (6.5')
Curtain	1m (3.25')
Animals	2m (6.5')

Table B.1: Recommended Mounting Height

Pet Immunity Guidelines

It is expected that the MS845 will eliminate false alarms caused by:

- Animals up to 45kg (PI)
- Several small rodents
- Random flying birds.

The weight of the animal should only be used as a guide, other factors s the length and color of fur also affect the level of immunity.

For maximum pet immunity the following guidelines are recommended:

- Mount the center of the unit at a height of 2m with the PCB vertical setting at -4.
- Set the pulse counter to 2.
- Do not aim the detector at stairways that can be climbed by an animal.
- Avoid a location where an animal can come within 1.8m of the detector by climbing on furniture, boxes or other objects.

INSTALLATION PROCEDURE

To install PIR sensors:

1. Open the housing by removing the front cover. To do so, insert a screwdriver in the release slot (located at the bottom of the detector between the front and back cover). Turn the screwdriver 90º to release the cover.
2. Remove the PCB by turning counter-clockwise and removing the Easy Lock – *do not touch the face of the pyro sensor!*
3. Apply battery power by removing the isolator that separates the battery from the contacts on the battery holder***. (Note: Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.)***
4. Place the Mode jumper over pins 2 & 3 (Radio Mode); the LED flashes.

Install the Mode jumper only after applying battery power.

5. From the Programming menu, select Devices, Zones [911].
6. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When ***Save?*** appears on the panel's LCD display, press ✓.
7. Remove the Mode jumper and place it over one pin for storage.
8. Choose an appropriate mounting height from Table B.1 and test the transmitter from the exact mounting position before permanently mounting the unit.
9. Knock out the mounting holes and attach the base to the wall.
10. Mount the PCB at the required vertical adjustment and replace the PCB screw.
11. Write the number of the zone on the sticker provided. Affix the sticker inside the front cover for future reference and replace the front cover.

Warm-Up Time

The detector will need to warm up for the first 90 seconds after applying power.

Pulse Counter

Switch 2	Switch 3	Pulse Count
OFF	OFF	1
ON	OFF	2
ON	ON	3
OFF	ON	Adaptive

Table B.3: Pulse Count Setting (MS845)

The pulse counter determines the amount of beams that need to be crossed before the detector will generate an alarm. To set the pulse counter, refer to table B.3.

Adaptive Pulse Count

Using the Adaptive pulse count feature, the detector chooses between 1 or 2 pulses based on its analysis of the received signal.

© MARMITEK

Vertical Adjustment

To position the PCB, turn the Easy Lock counter-clockwise and slide the PCB up or down to the required setting using the vertical adjustment scale. The detector's coverage area is 12m x 12m when the PCB is positioned at 0. Slide the PCB up towards the -8 position to decrease the coverage area bringing the beams closer to the mounting wall.

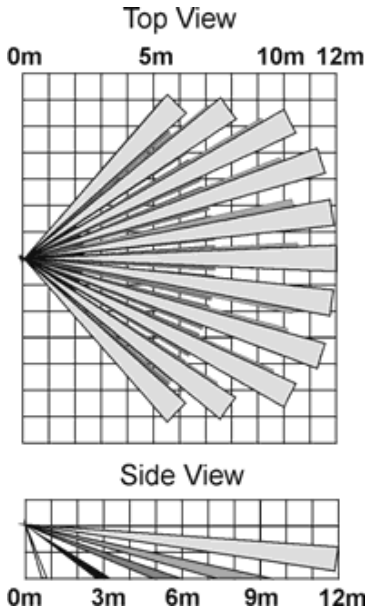


Figure B.2: Lens Coverage Diagrams

Walk Test Mode

A walk test is performed in order to determine the lens coverage pattern of the detector – *see Figure B.2*. Walk Test mode cancels the delay time between detections, enabling you to perform an efficient walk test.

To perform a Walk Test.

1. Place the Mode jumper over pins 1 & 2.
2. Walk across the scope of the detector according to the detection pattern selected.
3. Confirm that the LED activates and deactivates accordingly. Wait five seconds after each detection before continuing the test.
4. After completing the walk test, remove the jumper and place it over one pin for storage – *see Mode Jumper Safeguard*.

LED Indication

The LED indicator is lit twice every time a transmission is made. To enable or disable LED indication, refer to Table B.4 below.

LED Indication	MS845
Disabed	DIP-Switch 1 OFF
Enabled	DIP-Switch 1 ON

Table B.4: LED Indication Settings

The LED should only be disabled after successfully walk testing the detector.

Mode Jumper Safeguard

During normal operation, the Mode jumper should be placed over one pin for storage. When the mode jumper is placed over two pins, the detector is either in Radio or Walk Test Mode. As a precaution, these modes are limited to three minutes. After three minutes have expired, the detector switches back to normal operation. If this happens, you can reset a mode by removing and replacing the mode jumper.

Magnetic Contact (DS831)

The DS831 is a magnetic contact designed for installation on doors and windows.

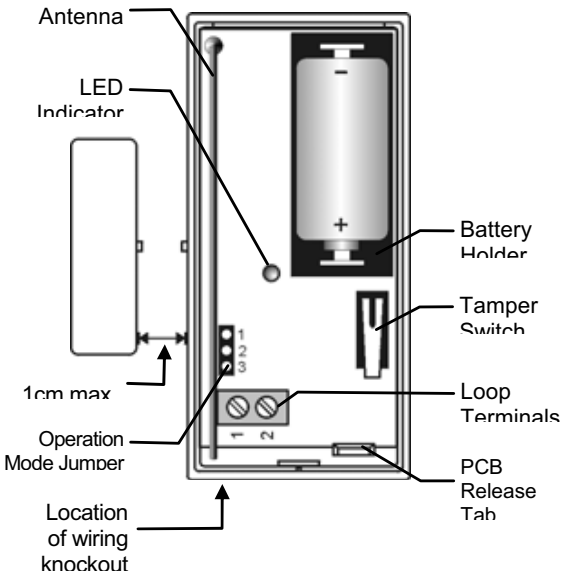


Figure B.3: DS831 (cover off)

INSTALLATION PROCEDURE

To install magnetic contacts.

1. To open the housing, insert a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
2. Remove the divider separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the DS831 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch.

Note: Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.

When handling the PCB, do not apply pressure on the antenna.

3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When ***Save?*** appears on the panel's LCD display, press ✓.
5. After registration, press the DS831's tamper switch to terminate Test mode.

Jumper Position	Operation Mode
Pins 1&2	Universal Transmitter
Pins 2&3	Magnetic Switch
Jumper Removed	Magnetic Switch/ Universal Transmitter

Table B.5: Operation Mode Jumper

6. Before permanently mounting the unit, test the transmitter from the exact mounting position.
7. To remove the PCB, press the PCB release tab and carefully lift the board and slide the board away from the back cover.
8. The DS831 is able to operate in three modes: Magnetic Switch, Universal Transmitter or a combination of the two. If connecting a wired contact loop (N.C.), connect the terminal block as follows: 1 - Alarm; 2 - GND. For this purpose, a wiring knockout is provided in the back cover.
9. Mount the back cover using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB – *see Figure B.4*.

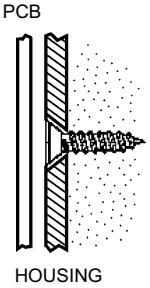


Figure B.4: Mounting Screw Position

10. To open the magnet's housing, insert a small screwdriver into one of the pry-off slots located at either end of the magnet's back cover and lift to separate from the front cover.

© MARMITEK

11. Mount the back cover of the magnet using two screws. Make sure that the guideline on the magnet is correctly aligned with the guideline on the transmitter.

Do not install the magnet further than 1cm from the transmitter.

12. Test the transmitter, making certain that the LED is lit when opening the door/window and again when closing.
13. Close the front covers of the transmitter and the magnet.

Universal Transmitter (US832)

The US832 is a universal transmitter that includes a single output for use in a wide range of wireless applications.

Installation Procedure

To install universal transmitters:

1. To open the housing, insert a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
2. Remove the divider separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the US832 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch. Test mode is automatically terminated after approximately five minutes.

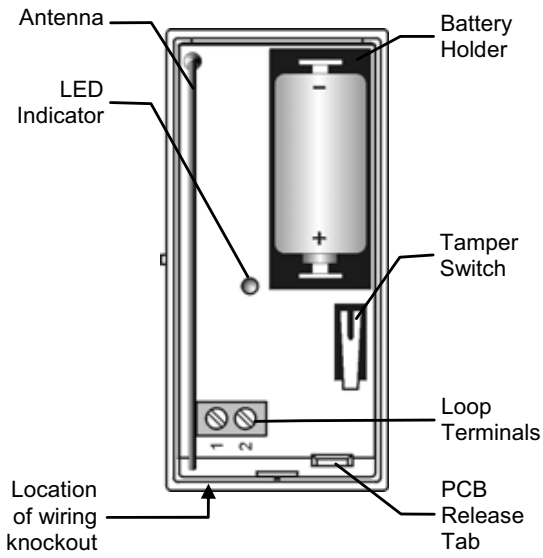


Figure B.5: US832 (cover off)

3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When ***Save?*** appears on the panel's LCD display, press ✓.
5. After registration, press the US832's tamper switch to terminate Test mode.
6. Before permanently mounting the unit, test the transmitter from the exact mounting position.
7. To remove the PCB, press the PCB release tab, carefully lift the board and slide the board away from the back cover.

When handling the PCB, do not apply pressure on the antenna.

8. Knockout the wiring hole in the back cover.
9. Thread the wires through the wiring hole.
10. Mount the back cover to the wall using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB – *see Figure B.4*.
11. Connect the terminal block as follows: 1 - Alarm; 2 - GND.
12. Test the transmitter, making certain that the LED is lit during transmissions.
13. Close the front cover of the US832.

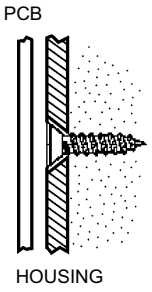


Figure B.4: Mounting Screw Position

© MARMITEK

Glass break Sensor (GB843)

The GB843 is an intelligent acoustic glass break sensor with an incorporated wireless transmitter.

Mounting Considerations

The GB843 acoustic sensor is omni-directional, providing 360º coverage. The coverage is measured from the sensor to the point on the glass farthest from the sensor. The sensor can be mounted as close as 1m from the glass.

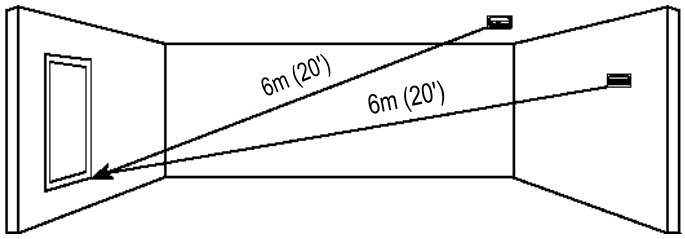


Figure B.6: Acoustic Sensor Range Measurement (plate, tempered, laminated and wired glass)

Sensor range:

- If mounting on the ceiling, the opposite wall or adjoining walls, the maximum range is 6m for plate, tempered, laminated and wired glass.
- For armor-coated glass, the maximum range is 3.65m.

Minimum recommended glass size:

- 0.3m x 0.6m

Glass thickness:

- Plate: 2.4mm to 6.4mm
- Tempered: 3.2mm to 6.4mm
- Wired: 6.4mm
- Laminated: 3.2mm to 6.4mm

For best detection:

- The sensor must always be in direct line of sight of all windows to be protected.
- If mounting on the wall, try to install the sensor directly opposite the protected window. If this is not possible, adjoining side walls are also a good location.
- If mounting on the ceiling, install the sensor 2-3m into the room.
- Avoid installing in rooms with lined, insulating or sound deadening drapes.
- Avoid installing in rooms with closed wooden window shutters inside.
- Avoid installing in the corners of a room.

The GB843 is best suited to rooms with moderate noise.

The sensor may not consistently detect cracks in the glass, bullets which break through the glass or glass breaking around corners and in other rooms. Glass break sensors should always be backed up by interior protection.

For best false alarm immunity:

- Locate the sensor at least 1.2m away from noise sources (televisions, speakers, sinks, doors, etc.).
- Avoid rooms smaller than 3m x 3m and rooms with multiple noise sources.
- Do not use where white noise, such as air compressor noise, is present (a blast of compressed air may cause a false alarm).

- Do not define the zone as 24hr. It is recommended to register the GB843 to a perimeter arming group that arms the perimeter doors and windows of the premises.
- Avoid humid rooms – the GB843 is not hermetically sealed. Excess moisture can eventually cause a short and a false alarm.

Areas to avoid:

- Glass airlocks and glass vestibule areas
- Noisy kitchens
- Residential car garages
- Small utility rooms
- Stairwells
- Small bathrooms
- Other small acoustically live rooms

For glass break protection in such applications, use shock sensors on the windows or window frames connected to an US832 universal transmitter.

Installation Procedure

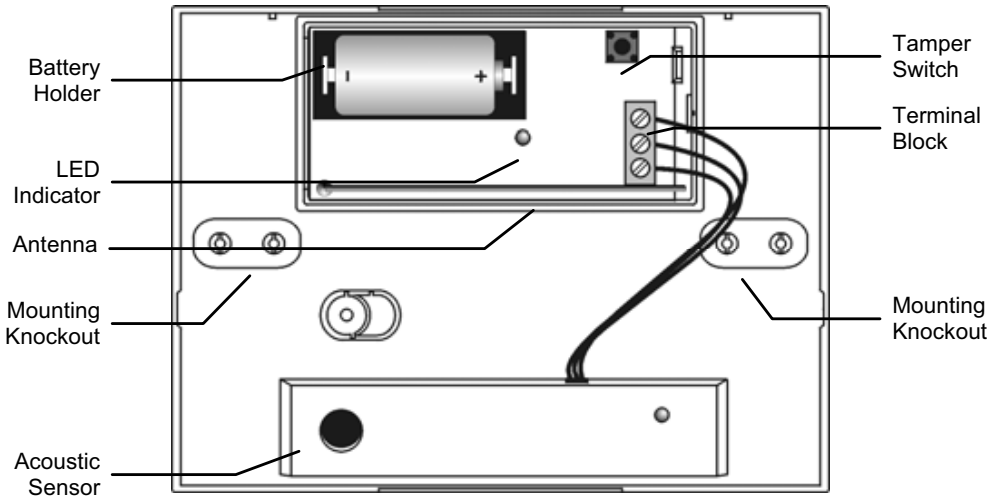


Figure B.7: GB843 (cover off)

1. Open the housing using a small flat-head screwdriver to separate the base from the cover.
2. Remove the insulator separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the GB843 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch. Test mode is automatically terminated after approximately five minutes.
3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When ***Save?*** appears on the panel's LCD display, press ✓.
5. After registration, press the GB843's tamper switch to terminate Test mode.
6. Choose a suitable mounting location according to the guidelines in the previous section.

© MARMITEK

7. Before permanently mounting the unit, test the acoustic sensor and the transmitter from the exact mounting position. For further information on testing the acoustic sensor, refer to the following section, Hand Clap Test.
8. Knock out the required mounting holes on the back cover.
9. Mount the unit to the wall using the mounting screws provided.
10. Write the number of the zone on the sticker provided and affix the sticker inside the front cover for future reference.
11. Close the front cover making sure that it snaps shut.

Hand Clap Test

The Hand Clap test enables you to test the GB843 while in Normal mode. This test checks the sensors power supply, microphone and circuit board.

To perform a Hand Clap test
Clap your hands loudly under the sensor; the LED flashes twice but an alarm is not generated.

Smoke Detector (SD833)

The SD833 is a brand-name smoke detector with an integrated Marmitek transmitter.

Installation Procedure

The following procedure explains the installation of the SD833 wireless smoke detector and its registration to the receiver. For further information regarding the smoke detector's location, test procedures, maintenance and specifications, refer to the manufacturer's installation instructions provided with this product.

To install smoke detectors:

1. Open the cover by lifting the opening tab while firmly holding the base with your other hand.
2. Push the cover backwards to separate the cover from the base.
3. Install a 9V battery into the detector's battery snap.
4. Insert the Test jumper; the SD833 enters Test mode and the LED flashes every few seconds.
5. From the Programming menu, select ***Devices, Zones*** [911].
6. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When ***Save?*** appears on the panel's LCD display, press ✓.
7. After registration, remove the Test jumper and place it over one pin for storage.
8. Before permanently mounting the unit, test the transmitter from the exact mounting position.
9. Attach the mounting base to the ceiling using the screws provided.
10. Replace the cover onto its hinges and close the cover until it snaps together with the base.

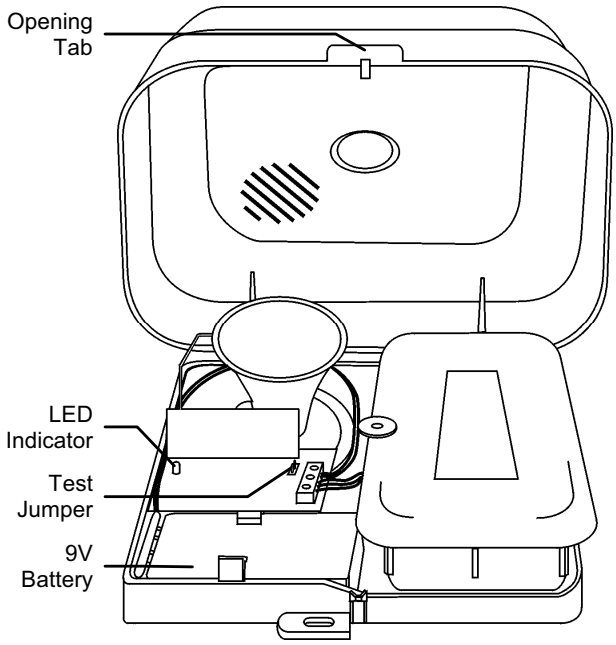


Figure B.9: SD833 (cover open)

© MARMITEK

Keyfobs (PR811/KR814)

The PR811 and KR814 are keyfob transmitters that are supported by the system.

REGISTRATION PROCEDURE

To register keyfobs:

1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the keyfob you want to register; the system initiates Registration mode.
3. Press a button, making sure that the keyfob's LED lights up when the button is pressed.
4. Press the same button again. When ***Save?*** appears on the panel's LCD display, press ✓.

PR811

The PR811 is a one-button transmitter that generates a Medical Emergency alarm when pressed. The transmitter is water resistant and can be worn around the neck. Its large button makes it ideal for elderly or sight-impaired users.

When the battery is low, the PR811's LED flashes during transmission and a Low Battery signal is sent to the receiver. When either of these two indications are observed, replace the unit.

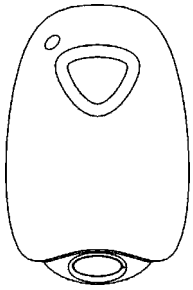


Figure B.10: PR811

Figure B.11: KR814

KR814

The KR814 is a four-button keyfob transmitter that offers a number of functions including arm, disarm and SOS Panic.

When the battery is low, the KR814's LED flashes during transmission and a Low Battery signal is sent to the receiver. When either of these two indications are observed, replace the batteries.

To replace the batteries:

1. Insert a small screwdriver into the pry-off slot – *see Figure B.12* Carefully twist the screwdriver to separate the front and back of the casing.
2. Observing correct polarity, replace the batteries (3V lithium, size: CR1225).
3. Close the casing making sure that the front and back click shut.

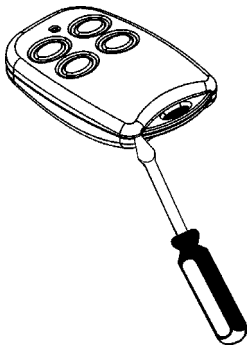


Figure B.12: Opening the KR814's Casing

Wireless Keypads (WK820/RC840)

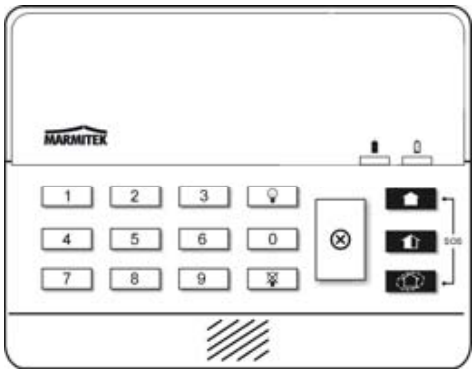


Figure B.13: WK820

INTRODUCTION

The WK820 and RC840 are one-way wireless keypads primarily designed as additional arming stations, including three arming keys that enable Full, Part or Perimeter arming modes. Pressing the Full and Perimeter buttons simultaneously generates an SOS panic alarm. Additionally, the keypad may be used to control Home Automation modules.

The WK820 also includes an additional Cancel key ⊗ that clears the keypad in the event that a key is pressed by mistake while entering a code, for example. This key causes the keypad to disregard what was previously entered enabling the user to start again.

REGISTRATION PROCEDURE

To register wireless keypads:

1. From the Programming menu, select Devices, Keypads [913].
2. Select the keypad you want to register; the system initiates Registration mode.
3. Press a button on the keypad making sure that a LED lights up when the button is pressed.
4. Press the same button again. When ***Save?*** appears on the panel's LCD display, press ✓.

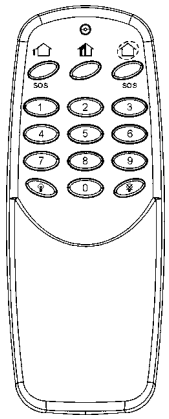


Figure B.14: RC840

BATTERY REPLACEMENT (WK820)

Every time a key is pressed, one of the battery status LEDs is lit. When the battery needs to be replaced, the red Low Battery LED is lit.

To replace the battery:

1. Insert a small screwdriver into the pry-off slots at the bottom of the unit and twist to remove the back cover.
2. Observing correct polarity, replace the battery (9V, alkaline).
3. Replace the back cover making sure that the two covers click shut.

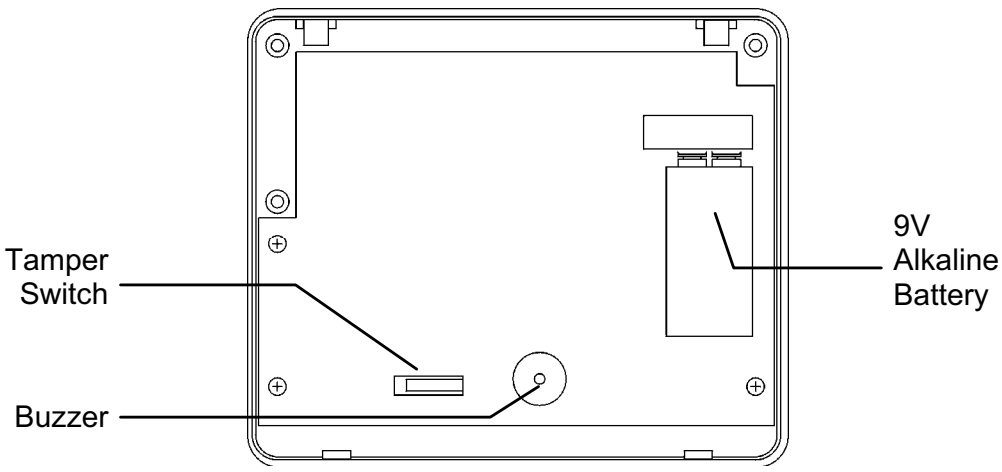


Figure B.15: WK820 (back cover off)

© MARMITEK

BATTERY REPLACEMENT (RC840)

When the battery is low, the RC840's LED flashes during transmission.

To replace the battery:

1. Remove the battery cover located at the rear of the unit. To do so, press the release tab using a small screwdriver and lift the cover away from the RC840's plastic housing.
2. Observing correct polarity, replace the battery (9V, alkaline).
3. Replace the battery cover making sure that it clicks shut.

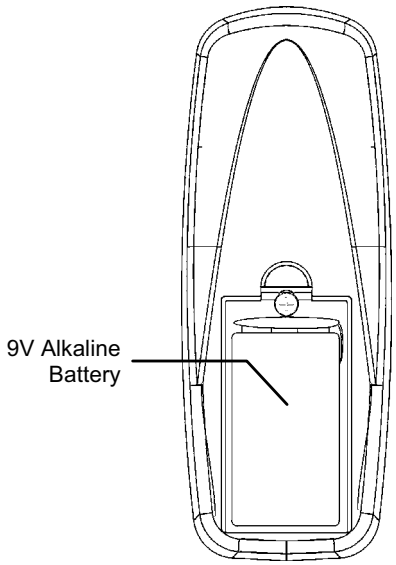


Figure B.16: RC840
(battery cover off)

Transmitter Specifications

The technical specifications for the transmitters that appear in this appendix are listed below. All transmitters are available in 868.35 MHz FM frequencies. Specifications may be modified without prior notice.

MS845

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 30mA (transmission),
6µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 12 x 12m
Pulse Count: 1, 2, 3 or Adaptive
LED Indicator: Selectable
Adaptive Temperature Compensation
RFI Immunity: 30V/m
Operating Temperature: -10 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 60 x 45mm

DS831/US832

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 25mA (transmission)
10µA (standby)
Loop Input Voltage Range: 0-15VDC/AC (peak to peak)
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 65 x 30 x 25mm

SD833

Antenna: Built-in Internal Whip
Current Consumption: 30mA (transmission),
20µA (standby)
Power: 9V Alkaline Battery
RFI Immunity: 40V/m
Ambient temperature: 0° C to + 60° C (operation)
Dimensions: 138 x 118 x 44mm

GB843

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 25mA (transmission)
30µA (standby)
Microphone: Omni-directional electret
Maximum Range: 6m (plate, tempered, laminated and wired glass)
3.65m (armor-coated glass)
RFI Immunity: 20V/m
Operating Temperature: 0 to 50°C
Dimensions: 80 x 108 x 43mm

PR811

Antenna: Built-in Whip
Power: Non-replaceable battery
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 60 x 40 x 15mm

KR814

Antenna: Built-in Whip
Power: 2 x 3V Lithium Battery Size CR1225
Current Consumption: 16mA (transmission)
2µA (standby)
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 62 x 42 x 15mm

WK820

Antenna: Printed on PCB
Current Consumption: 26mA (transmission)
2µA (standby)
Power: 9V Alkaline Battery
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 130 x 110 x 28mm

RC840

Antenna: Printed on PCB
Current Consumption: 25mA (transmission)
3µA (standby)
Power: 9V Alkaline Battery
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 128 x 49 x 27mm

© MARMITEK

Appendix C: Event Table

Burglary

Description	🔧	Restore	SIA	Contact ID	Address Field
Alarm from Zone			NBA	1130	Device Number
Zone Alarm Restore	◆	◆	NBR	3130	Device Number
Zone Bypassed			NUB	1570	Device Number
Zone Unbypassed	◆	◆	NUU	3570	Device Number
Zone Tamper			NTA	1137	Device Number
Zone Tamper Restore	◆	◆	NTR	3137	Device Number
Zone Panic Alarm			NPA	1120	Device Number
Zone Panic Restore	◆	◆	NPR	3120	Device Number
Panic Alarm			NPA	1120	Device Number
Tamper			NTA	1137	Device Number
Tamper Restore	◆	◆	NTR	3137	Device Number
Duress			NHA	1121	—
Bell Cancel	◆		NBC	1521	User Number
Disarm after Alarm			NOR	1458	User Number
Water Alarm			NWA	1154	Device Number
Water Alarm Restore	◆	◆	NWH	3154	Device Number
Environmental Alarm			NUA	1150	Device Number
Environmental Alarm Restore	◆	◆	NUH	3150	Device Number
Alarm Cancel			NOC	1406	User Number

Fire

Fire Alarm			NFA	1110	Device Number
Fire Alarm Restore	◆	◆	NFR	3110	Device Number
Gas Alarm			NGA	1151	Device Number
Gas Alarm Restore	◆	◆	NGH	3151	Device Number

Open/Close

Full Arm			NCL	3401	User Number
Part Arm			NCG	3456	User Number
Perimeter Arm			NCG	3441	User Number
Disarm			NOP	1401	User Number

Service

Edit User Code	◆		NJV	1462	User Number
Delete User Code	◆		NJX	3462	User Number
System Programming	◆		NLB	1627	—
End System Programming	◆		NLX	1628	—
Remote Programming	◆		NRB	1412	—
End Remote Programming	◆		NRS	3412	—
Walk Test	◆		NTS	1607	User Number
End Walk Test	◆		NTE	3607	—
Set Time	◆		NJT	1625	User Number
Set Date	◆		NJD	1625	User Number
Clear Log			NLB	1621	User Number

🔧 = Events that are displayed in the event log only when viewed by the installer.

Power

Description	🔧	Restore	SIA	Contact ID	Address Field
Battery Low			NYT	1302	Device Number
Battery Restore		◆	NYR	3302	Device Number
Transmitter Low Battery			NXT	1384	Device Number
Transmitter Battery Restore		◆	NXR	3384	Device Number
AC Loss			NAT	1301	Device Number
AC Restore		◆	NAR	3301	Device Number

Peripherals

Media Loss			NLT	1351	Device Number
Media Loss Restore	◆	◆	NLR	3351	Device Number
Device Trouble			NET	1330	Device Number
Device Trouble Restore	◆	◆	NER	3330	Device Number
Transmitter Out of Synch.			NUT	1341	Device Number
Transmitter Re-synch.	◆	◆	NUR	3341	Device Number
CP Transmitter Out of Synch.			NUT	1341	Device Number
CP Transmitter Re-synch.	◆	◆	NUR	3341	Device Number
Supervision Loss			NUS	1381	Device Number
Supervision Restore	◆	◆	NUR	3381	Device Number
GSM Signal Level	◆		NYY	1605	Signal Level (0-9)
Zone Trouble			NBT	1380	Device Number
Zone Trouble Restore	◆	◆	NBJ	3380	Device Number

RF Jamming

FM Jamming			NXQ	1344	Device Number
FM Jamming Restore	◆	◆	NXH	3344	Device Number

Medical

Medical Alarm			NMA	1100	Device Number
Medical Alarm Restore	◆	◆	NMR	3100	Device Number
No Motion			NNA	1102	Device Number

Unclassified Events

Periodic Test	◆		NRP	1602	—
No Arm	◆		NCD	1654	—

Address Field

The address field provides additional information regarding the event. This information is forwarded as numeric data according to the following tables.

DEVICE NUMBER	
Value	**Description**
00	Control Panel
01-32	Wireless Zones
33	Hardwire Zone
41-59	Keyfobs
65	Home Automation Module
77-80	Repeaters
81-84	Wireless Keypads
91	Front Panel Keypad
92-98	Hardwire Keypads
110	Wireless Siren
243	PSTN Module
244	Cellular Communications Module

USER NUMBER	
Value	**Description**
00	Control Panel
01-32	Users
34	Remote Access
41-59	Keyfobs
61-76	Smartkeys
81-84	Wireless Keypads
91	Front-panel Keypad
92-98	Hardwire Keypads

Appendix D: Zone Types

Normal

A Normal zone is active when the system is armed. This zone generates a Burglary alarm instantly when triggered. Normal zones are designed for detectors installed inside the protected site or doors/windows that are never used to enter the premises.

Event Group: Burglary

Entry/Exit

When the system is armed, Entry/Exit zones initiates the entry delay when triggered. If the system is not disarmed by the time the entry delay expires, a Burglary alarm is generated. These zones are designed for detectors protecting the entrance to the protected site

Event Group: Burglary

Follower

If an Entry/Exit zone is triggered first, Follower zones do not generate an alarm when triggered during the entry delay. If the system is not disarmed by the end of the entry delay, the Follower zone generates an alarm. A Follower zone instantly generates an alarm if triggered when the entry delay is not active. These zones are designed for detectors protecting the area in which a keypad has been installed or the area crossed in order to reach the keypad.

Event Group: Burglary

Panic

Panic zones are always active. When a Panic zone is triggered, a Panic alarm is generated. This zone type is designed for panic buttons that may be pressed in a hold-up situation. If the Bell option is disabled for Panic zones, in addition to the siren not sounding, all forms of alarm indication from the keypad are also disabled.

Event Group: Burglary

Medical

Medical zones are always active. When triggered, Medical zones generate a Medical alarm. These zones are used typically with panic buttons that may be pressed in the event of a medical emergency.

Event Group: Medical

Fire

Fire zones are always active. When triggered, Fire zones generate a Fire alarm. These zones are designed for use with smoke detectors and panic buttons that may be pressed in the event of a fire. A Fire zone always activates the siren even if the Bell option is programmed as disabled. Fire alarms sound a pulsating siren to distinguish them from other alarms.

Event Group: Fire

24Hr

24Hr zones are always active. When triggered, 24Hr zones generate a Burglary alarm. These zones are used for applications that require constant protection.

Event Group: Burglary

24Hr-X

The 24Hr-X zone is a future option that is not available in the current firmware.

Event Group: Not applicable

Gas

Gas zones are always active. In the event of a gas leak, these zones generate a Gas alarm. Gas zones are typically used with methane/propane/butane or carbon monoxide gas detectors. Gas alarms sound a distinctive siren pattern to easily distinguish them from other alarms. A gas alarm causes the siren to sound until the alarm is restored; the siren cut-off does not apply to gas alarms.

Event Group: Fire

Flood

Flood zones are always active. When triggered, Flood zones generate a Water alarm. These zones are designed for use with WD861 flood sensors.

Event Group: Burglary

Environmental

Environmental zones are always active. When triggered, these zones generate an Environmental alarm. These zones are designed for applications that monitor environmental conditions such as temperature or humidity. If the Bell option is enabled for Environmental zones, the system sounds trouble tones from the keypad. These tones are sounded until the user presses ▼ on their keypad. Environmental alarms are not affected by the expiry of the siren cut-off.

Event Group: Burglary

No Motion

No Motion zones are used to monitor the activity of disabled or elderly people. If a No Motion zone has not been triggered within a pre-defined period of time (6, 12, 24, 48 or 72 hours), a No Motion event message is sent to the monitoring station.

Event Group: Medical

Not Used

This zone type disables the sensor output. All alarm transmissions from the sensor are ignored though the sensor may still be used to activate HA units in Home Automation applications.

Event Group: Not applicable

Declaration of Conformity

Hereby, Marmitek BV, declares that this PROGUARD800 is in compliance with the essential requirements and other relevant provisions of the following Directives:

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits

868.35MHz is not intended for use in BG, GR, PL & SI.

Environmental Information for Customers in the European Union
European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Copyrights

Marmitek is a trademark of Marmidenko B.V. | ProGuard800 is a trademark of Marmitek B.V. All rights reserved.

Copyright and all other proprietary rights in the content (including but not limited to model numbers, software, audio, video, text and photographs) rests with Marmitek B.V. Any use of the Content, but without limitation, distribution, reproduction, modification, display or transmission without the prior written consent of Marmitek is strictly prohibited. All copyright and other proprietary notices shall be retained on all reproductions.

MARMITEK®

www.marmitek.com

ZI0488A (4-07)